ESET SMART SECURITY 9

Guia do Usuário

(destinado ao produto versão 9,0 e posterior)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Clique aqui para fazer download da versão mais recente deste documento

ESET SMART SECURITY

Atendimento ao cliente mundial www.eset.com/support

REV. 10/6/2015

Índice

Índice

1. ESET Smart Security

O ESET Smart Security representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ThreatSense®, combinada com o firewall pessoal personalizado e os módulos antispam, utiliza velocidade e precisão para manter o computador seguro. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

O ESET Smart Security é uma solução de segurança completa que combina proteção máxima e impacto mínimo no sistema. Nossas tecnologias avançadas usam inteligência artificial para impedir infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outras ameaças sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

Recursos e benefícios

Interface do usuário com novo design	A interface do usuário na versão 9 foi redesenhada e simplificada significativamente com base em resultados de testes de usabilidade. Toda a linguagem da interface gráfica do usuário e das notificações foi revisada cuidadosamente e a interface agora é compatível com idiomas da direita para a esquerda, como hebreu e árabe. **Ajuda on-line** agora está integrada ao ESET Smart Security e oferece um conteúdo de suporte dinamicamente atualizado.
Antivírus e antispyware	Detecta e limpa proativamente mais vírus, worms, cavalos de troia e rootkits conhecidos e desconhecidos. A **heurística avançada** sinalizada até mesmo malware nunca visto antes, protegendo você de ameaças desconhecidas e neutralizando-as antes que possam causar algum dano. A **proteção de acesso à Web** e **proteção antiphishing** funcionam monitorando a comunicação entre os navegadores da Internet e servidores remotos (incluindo SSL). A **Proteção do cliente de email** fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP.
Atualizações regulares	Atualizar o banco de dados de assinatura de vírus e os módulos do programa periodicamente é a melhor forma de garantir o nível máximo de segurança em seu computador.
ESET LiveGrid® (Reputação potencializada pela nuvem)	Você pode verificar a reputação dos arquivos e dos processos em execução diretamente do ESET Smart Security.
Controle de dispositivos	Rastreia automaticamente todas as unidades flash USB, cartões de memória e CDs/DVDs. Bloqueia mídia removível com base no tipo de mídia, fabricante, tamanho e outros atributos.
Funcionalidade do HIPS	Você pode personalizar o comportamento do sistema em mais detalhes; especifique regras para o registro do sistema, processos e programas ativos e ajuste sua postura de segurança.
Modo jogador	Adia todas as janelas pop-up, atualizações ou outras atividades que exijam muitos recursos do sistema, a fim de conservar recursos do sistema para jogos e outras atividades de tela inteira.

Recursos no ESET Smart Security

Proteção de Atividade bancária e Pagamento	A proteção de Atividade bancária e Pagamento fornece um navegador seguro a ser usado ao acessar gateways de atividade bancária ou pagamento on-line para garantir que todas as atividades on-line acontecem em um ambiente confiável e seguro.

Suporte para assinaturas de rede	Assinaturas de rede permitem a identificação e bloqueio rápido de tráfego malicioso vindo de e para dispositivos de usuários como bots e pacotes de exploit. O recurso pode ser considerado uma melhoria da Proteção contra botnet.
Firewall inteligente	Impede que usuários não autorizados acessem seu computador e utilizem seus dados pessoais.
ESET Antispam	Os spams representam até 80 por cento de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema.
ESET Antifurto	o ESET Antifurto expande a segurança no nível de usuário no caso de um computador roubado ou perdido. Quando os usuários instalarem o ESET Smart Security e o ESET Antifurto, seu dispositivo será relacionado na interface da web. A interface da web permite que os usuários gerenciem sua configuração do ESET Antifurto e administrem recursos antifurto em seu dispositivo.
Controle dos pais	Protege sua família contra conteúdo na Web potencialmente ofensivo bloqueando várias categorias de sites.

Uma licença precisa estar ativa para que os recursos do ESET Smart Security estejam operacionais. Recomenda-se que você renove sua licença várias semanas antes de a licença do ESET Smart Security expirar.

1.1 Novidades da versão 9

ESET Smart Security versão 9 contém as melhorias a seguir:

- **Proteção de Atividade bancária e Pagamento** - Uma camada de proteção adicional para transações on-line.
- **Suporte para assinaturas de rede** - Assinaturas de rede permitem a identificação e bloqueio rápido de tráfego malicioso vindo de e para dispositivos de usuário relacionados a bots e pacotes de exploit.
- **Interface do usuário com novo design** - A interface gráfica do usuário do ESET Smart Security foi totalmente reformulada para fornecer melhor visibilidade e uma experiência mais intuitiva para o usuário. A interface agora é compatível com idiomas da direita para a esquerda, como hebreu e árabe. **Ajuda on-line** agora está integrada ao ESET Smart Security e oferece um conteúdo de suporte dinamicamente atualizado.
- **Instalação mais rápida e confiável** - Incluindo um rastreamento inicial executado automaticamente 20 minutos após a instalação ou reinicialização.

Para mais detalhes sobre os novos recursos no ESET Smart Security, leia o seguinte artigo na Base de conhecimento ESET:
O que há de novo no ESET Smart Security 9 e ESET NOD32 Antivírus 9?

1.2 Requisitos do sistema

Para uma operação sem interrupções do ESET Smart Security, o sistema deve atender aos seguintes requisitos de hardware e de software:

Processadores compatíveis: Intel® ou AMD x86-x64
Sistemas operacionais: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit/Home Server 2003 SP2 32-bit/Home Server 2011 64-bit

1.3 Prevenção

Quando você trabalhar com o computador, e especialmente quando navegar na Internet, tenha sempre em mente que nenhum sistema antivírus do mundo pode eliminar completamente o risco de infiltrações e ataques. Para fornecer proteção e conveniência máximas, é essencial usar a solução antivírus corretamente e aderir a diversas regras úteis:

Atualização regular

De acordo com as estatísticas do ThreatSense, milhares de novas ameaças únicas são criadas todos os dias a fim de contornar as medidas de segurança existentes e gerar lucro para os seus autores - todas às custas dos demais usuários. Os especialistas no Laboratório de pesquisa da ESET analisam essas ameaças diariamente, preparam e publicam atualizações a fim de melhorar continuamente o nível de proteção de nossos usuários. Para garantir a máxima eficácia dessas atualizações, é importante que elas sejam configuradas devidamente em seu sistema. Para obter mais informações sobre como configurar as atualizações, consulte o capítulo Configuração da atualização.

Download dos patches de segurança

Os autores dos softwares maliciosos frequentemente exploram as diversas vulnerabilidades do sistema a fim de aumentar a eficiência da disseminação do código malicioso. Considerado isso, as empresas de software vigiam de perto quaisquer vulnerabilidades em seus aplicativos para elaborar e publicar atualizações de segurança, eliminando as ameaças em potencial regularmente. É importante fazer o download dessas atualizações de segurança à medida que são publicadas. Microsoft Windows e navegadores da web, como o Internet Explorer, são dois exemplos de programas para os quais atualizações de segurança são lançadas regularmente.

Backup de dados importantes

Os escritores dos softwares maliciosos não se importam com as necessidades dos usuários, e a atividade dos programas maliciosos frequentemente leva ao mau funcionamento de um sistema operacional e a ´perda de dados importantes. É importante fazer o backup regular dos seus dados importantes e sensíveis para uma fonte externa como um DVD ou disco rígido externo. Isso torna mais fácil e rápido recuperar os seus dados no caso de falha do sistema.

Rastreie regularmente o seu computador em busca de vírus

A detecção de mais vírus, cavalos de troia e rootkits conhecidos e desconhecidos é realizada pelo módulo Proteção em tempo real do sistema de arquivos. Isso significa que sempre que você acessar ou abrir um arquivo, ele será rastreado quanto à atividade de malware. Recomendamos que você execute um rastreamento no computador inteiro pelo menos uma vez por mês, pois a assinatura de malware varia, assim como as atualizações do banco de dados de assinatura de vírus são atualizadas diariamente.

Siga as regras básicas de segurança

Essa é a regra mais útil e eficiente de todas - seja sempre cauteloso. Hoje, muitas ameaças exigem a interação do usuário para serem executadas e distribuídas. Se você for cauteloso ao abrir novos arquivos, economizará tempo e esforço consideráveis que, de outra forma, seriam gastos limpando as ameaças. Aqui estão algumas diretrizes úteis:

- Não visite sites suspeitos com inúmeras pop-ups e anúncios piscando.
- Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Use somente programas seguros e somente visite sites da Internet seguros.
- Seja cauteloso ao abrir anexos de e-mail, especialmente aqueles de mensagens spam e mensagens de remetentes desconhecidos.
- Não use a conta do Administrador para o trabalho diário em seu computador.

2. Instalação

Há vários métodos para a instalação do ESET Smart Security em seu computador. Os métodos de instalação podem variar dependendo do país e meio de distribuição:

- O instalador Live pode ser obtido por download do site da ESET. O pacote de instalação é universal para todos os idiomas (escolha um idioma desejado). O próprio instalador Live é um arquivo pequeno; arquivos adicionais necessários para instalar o ESET Smart Security serão baixados automaticamente.

- Instalação off-line - Este tipo de instalação é uasdo ao instalar de um CD/DVD do produto. Ele usa um arquivo *.msi*, que é maior do que o arquivo do instalador Live e não exige uma conexão com a Internet ou arquivos adicionais para a conclusão da instalação.

Importante: Verifique se não há algum outro programa antivírus instalado no computador antes de instalar o ESET Smart Security. Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso artigo da base de conhecimento da ESET para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).

2.1 Instalador Live

Assim que você tiver feito download do pacote de instalação do *Instalador Live*, dê um duplo clique no arquivo de instalação e siga as instruções passo a passo na janela do instalador.

Importante: Para esse tipo de instalação, você deverá estar conectado à Internet.

Selecione seu idioma desejado no menu suspenso e clique em **Avançar**. Aguarde alguns momentos para o download dos arquivos de instalação.

Depois de aceitar o **Contrato de licença para o usuário final**, será solicitado que você configure o **ESET LiveGrid®**. O ESET LiveGrid® ajuda a assegurar que a ESET seja informada continua e imediatamente sobre novas infiltrações para proteger seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de pesquisa da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus.

Por padrão, **Desejo participar do ESET LiveGrid® (recomendado)** está selecionada, o que ativará esse recurso.

A próxima etapa do processo de instalação é a configuração da detecção de aplicativos potencialmente não desejados. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Consulte o capítulo Aplicativos potencialmente indesejados para obter mais detalhes.

Clique em **Instalar** para iniciar o processo de instalação.

2.2 Instalação off-line

Assim que você iniciar o pacote de instalação off-line (.msi), o assistente de instalação o guiará pelo processo de configuração.

Primeiro, o programa verifica para ver há uma versão mais nova do ESET Smart Security disponível. Se uma versão mais recente for encontrada, você será notificado na primeira etapa do processo de instalação. Se selecionar a opção **Fazer download e instalar nova versão**, a nova versão será obtida por download e a instalação continuará. Esta caixa de seleção só é visível quando há uma versão disponível mais recente do que a versão que você está instalando.

Em seguida, o Contrato de licença de usuário final será exibido. Leia-o e clique em **Aceitar** para confirmar a sua aceitação do Contrato de licença de usuário final. Depois que você aceitar, a instalação continuará.

Para obter mais instruções sobre etapas de instalação, o **ThreatSense** e **Detecção de aplicativos potencialmente indesejados**, siga as instruções na seção mencionada anteriormente (consulte "Instalador Live").

eset SMART SECURITY 9

Quanto mais melhor. Obtenha o nível máximo de proteção.

O sistema de feedback do ESET LiveGrid® nos permite coletar informações sobre objetos suspeitos, que processamos automaticamente para criar mecanismos de detecção em nosso sistema de nuvem. Em seguida eles são aplicados imediatamente para garantir que nossos clientes tenham o nível máximo de proteção.

☑ Ativar o sistema de feedback ESET LiveGrid® (recomendado)

Detecção de aplicativos potencialmente não desejados

A ESET pode detectar aplicativos potencialmente não desejados e pedir uma confirmação antes que eles sejam instalados. Aplicativos potencialmente indesejados podem não oferecer riscos de segurança, mas podem afetar o desempenho, a velocidade e a confiabilidade do computador, ou causar mudanças no seu comportamento. Normalmente eles pedem o consentimento do usuário antes da instalação.

Por exemplo, eles podem alterar suas configurações de página da web do navegador ou de pesquisa.

○ Desativar detecção de aplicativos potencialmente não desejados
○ Ativar detecção de aplicativos potencialmente não desejados

Instalar | Voltar | Alterar a pasta de instalação

2.2.1 Configurações avançadas

Após selecionar **Configurações avançadas**, será preciso definir um local para a instalação. Por padrão, o programa é instalado no seguinte diretório:

C:\Program Files\ESET\ESET Smart Security

Clique em **Procurar...** para alterar o local (não recomendado).

Clique em **Próximo** para configurar sua conexão com a Internet. Se você usa um servidor proxy, ele deve ser configurado corretamente para que as atualizações das assinaturas de vírus funcionem. Se você não tiver certeza se deve usar um servidor proxy para se conectar à Internet, selecione **Utilizar as mesmas configurações que o Internet Explorer (Recomendado)** e clique em **Próximo**. Se você não utilizar um servidor proxy, selecione **Eu não utilizo um servidor proxy**.

Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Próximo**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **usuário** e uma **senha** válidos a fim de obter acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Para fazer isso, clique em **Aplicar** e confirme a seleção.

A instalação personalizada permite definir como as atualizações automáticas do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as Configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes de programa**. Selecione **Perguntar antes de fazer download dos componentes de programa** para exibir uma janela de confirmação sempre que o sistema tentar fazer download dos componentes de programa. Para fazer download automaticamente de atualizações dos componentes do programa, selecione a opção **Sempre atualizar componentes do programa**.

OBSERVAÇÃO: Após a atualização dos componentes do programa, geralmente é necessária a reinicialização do sistema. Recomendamos selecionar **Se necessário, reiniciar o computador sem notificar**.

A próxima janela da instalação oferecerá a opção de definir uma senha para proteger as configurações do programa. Selecione **Proteger as configurações por senha** e digite a sua senha nos campos **Nova senha** e **Confirmar nova senha**. Esta senha será solicitada em todas modificações ou acessos futuros no ESET Smart Security. Quando ambos os campos de senha coincidirem, clique em **Próximo** para continuar.

Para concluir as próximas etapas de instalação, **ThreatSense** e **Detecção de aplicativos potencialmente não**

desejados, siga as instruções na seção Instalador Live (consulte "Instalador Live").

Em seguida, selecione um modo de filtragem para o firewall pessoal da ESET. Quatro modos de filtragem estão disponíveis para o firewall pessoal do ESET Smart Security. O comportamento do firewall é alterado com base no modo selecionado. Os Modos de filtragem também influenciam o nível de interação necessário do usuário.

Para desativar o primeiro rastreamento após a instalação que normalmente é realizado quando a instalação termina para verificar se há algum código malicioso, desmarque a caixa de seleção ao lado de **Ativar o rastreamento após a instalação**. Clique em **Instalar** na janela **Pronto para instalar** para concluir a instalação.

2.3 Problemas comuns de instalação

Se acontecer um problema durante a instalação, veja nossa lista de erros e soluções comuns de instalação para encontrar uma solução para seu problema.

2.4 Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos disponíveis para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país e meios de distribuição (CD/DVD, página da web da ESET etc.):

- Se Se você tiver adquirido uma versão do produto em uma caixa no varejo, ative o produto usando uma **Chave de licença**. A Chave de licença está normalmente localizada no interior ou na parte posterior da embalagem do produto. Para uma ativação bem-sucedida, a Chave de licença deve ser digitada conforme fornecida. Chave de licença - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX ou XXXX-XXXXXXXX que é usada para identificação do proprietário da licença e para ativação da licença.
- Se desejar avaliar o ESET Smart Security antes de fazer uma aquisição, selecione a opção **Licença de avaliação gratuita**. Insira seu endereço de email e país para ativar o ESET Smart Security por um período limitado. A licença de teste será enviada para seu email. As licenças de avaliação podem ser ativadas apenas uma vez por cliente.
- Se você não tem uma licença e deseja adquirir uma, clique em Comprar licença. Isso o redirecionará para o site do seu distribuidor local da ESET.

Selecione **Ativar mais tarde** se pretender avaliar rapidamente o nosso produto e não desejar ativá-lo imediatamente, ou se desejar ativar o produto depois.

Você pode ativar sua cópia do ESET Smart Security diretamente a partir do programa. Clique com o botão direito em no ícone do ESET Smart Security na bandeja do sistema e selecione **Ativar produto** no Menu do programa.

2.5 Digitando a Chave de licença

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Essa ação somente será possível se a **Chave de licença** correta for inserida na **Configuração da atualização**.

Se você não inseriu sua chave de licença durante a instalação, poderá inseri-la agora. Na janela principal do programa, clique em **Ajuda e suporte** depois em **Ativar licença** e insira os dados da licença recebidos com o produto de segurança ESET na janela Ativação do produto.

Ao digitar sua **Chave de licença**, é importante digitar exatamente como ela está escrita:

- Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usada para identificação do proprietário da licença e para ativação da licença.

Recomendamos que copie e cole sua chave de licença do seu email de registro para garantir a precisão.

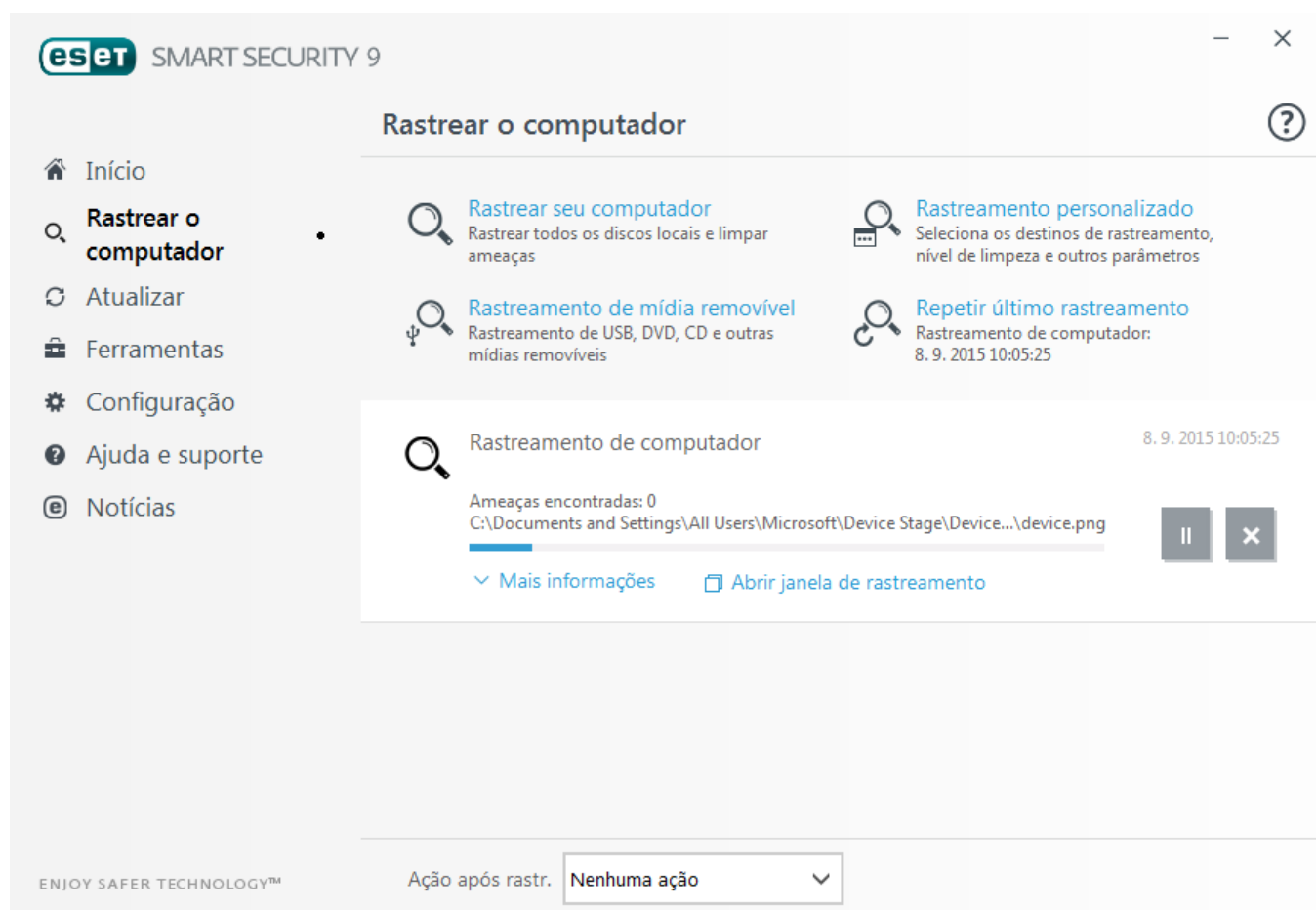
2.6 Atualização para uma versão mais recente

Versões mais recentes do ESET Smart Security são lançadas para implementar aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos do programa. A atualização para uma versão mais recente pode ser feita de várias formas:

1. Automaticamente, por meio de uma atualização do programa
   Como a atualização do programa é distribuída para todos os usuários e pode ter impacto em determinadas configurações do sistema, ela é lançada depois de um longo período de testes para garantir funcionalidade com todas as configurações de sistema possíveis. Se você precisar atualizar para uma versão mais recente imediatamente após ela ter sido lançada, use um dos métodos a seguir.
2. Manualmente na janela do programa principal, clicando em **Verificar se há atualizações** na seção **Atualizar**.
3. Manualmente, por meio de download e instalação de uma versão mais recente sobre a instalação anterior.

2.7 Primeiro rastreamento depois da instalação

Depois de instalar o ESET Smart Security, um rastreio de computador vai começar 20 minutos depois da instalação ou quando o computador reiniciar para verificar em busca de código malicioso.

Você também pode iniciar um rastreamento no computador manualmente a partir da janela principal do programa, clicando em **Rastreamento do computador** > **Rastrear seu computador**. Para obter mais informações sobre os rastreamentos do computador, consulte a seção Rastreamento do computador.

3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Smart Security e de suas configurações básicas.

3.1 Janela do programa principal

A janela principal do ESET Smart Security é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

Início - Fornece informações sobre o status da proteção do ESET Smart Security.

Rastreamento do computador - Configure e inicie um rastreamento do seu computador ou crie um rastreamento personalizado.

Atualizar - Exibe informações sobre as atualizações do banco de dados de assinatura de vírus.

Ferramentas - Fornece acesso a arquivos de log, estatísticas de proteção, monitoramento de atividade, processos em execução, conexões de rede, Agenda, ESET SysInspector e ESET SysRescue.

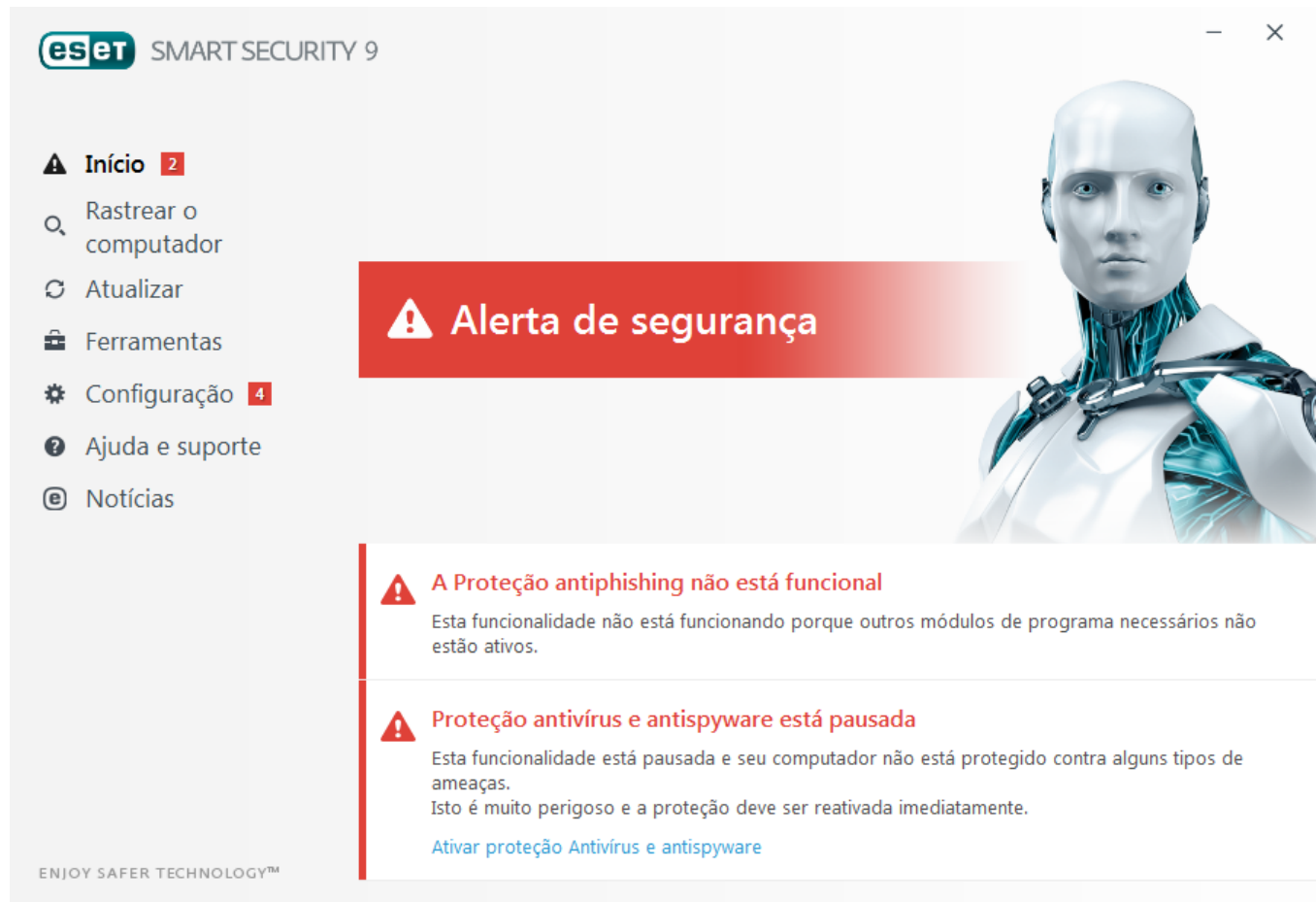
Configuração - Selecione essa opção para ajustar o nível de segurança para seu computador, internet, Proteção de rede e Ferramentas de segurança.

Ajuda e suporte – Fornece acesso aos arquivos de ajuda, Base de conhecimento ESET, ao site da ESET e a links para enviar uma solicitação de suporte.

A tela de **Início** contém informações importantes sobre o nível de proteção atual do seu computador. A janela de status também exibe os recursos mais usados do ESET Smart Security. Também é possível encontrar aqui informações sobre a atualização mais recente e a data de expiração do seu programa.

O ícone verde e status de **Proteção máxima** verde indica que a proteção máxima está garantida.

O que fazer se o programa não funcionar adequadamente?

Se um módulo de proteção ativa estiver funcionando corretamente, seu ícone do status de proteção estará verde. Um ponto de exclamação vermelho ou um ícone de notificação laranja indica que a máxima proteção não está garantida. Serão exibidas informações adicionais sobre o status de proteção de cada módulo, bem como soluções sugeridas para a restauração da proteção total em **Início**. Para alterar o status de módulos individuais, clique em **Configuração** e selecione o módulo desejado.

O ícone vermelho e o status vermelho Proteção máxima não garantida indicam problemas críticos. Há várias razões para esse status poder ser exibido, por exemplo:

- **Produto não ativado** - É possível ativar o ESET Smart Security no **Início** clicando em **Ativar produto** ou **Comprar agora** no Status da proteção.
- **O banco de dados de assinatura de vírus está desatualizado** - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o banco de dados de assinatura de vírus. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou as definições incorretas das configurações de conexão.
- **Proteção antivírus e antispyware desativada** - você pode reativar a proteção antivírus e antispyware clicando em **Iniciar todos os módulos de proteção antivírus e antispyware**.
- **Firewall pessoal ESET desativado** - Esse problema também é indicado por uma notificação de segurança próxima ao item **Rede**. Você pode reativar a proteção da rede clicando em **Ativar firewall**.
- **Licença expirada** - Isso é indicado pelo ícone do status de proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Siga as instruções da janela de alerta para renovar sua licença.

O ícone laranja indica proteção limitada. Por exemplo, pode haver um problema com a atualização do programa ou a data de expiração da sua licença está se aproximando.
Há várias razões para esse status poder ser exibido, por exemplo:

- **Alerta de otimização Antifurto** - este dispositivo não está otimizado para o ESET Antifurto. Por exemplo, uma Conta fantasma (um recurso de segurança que é acionado automaticamente quando você marca um

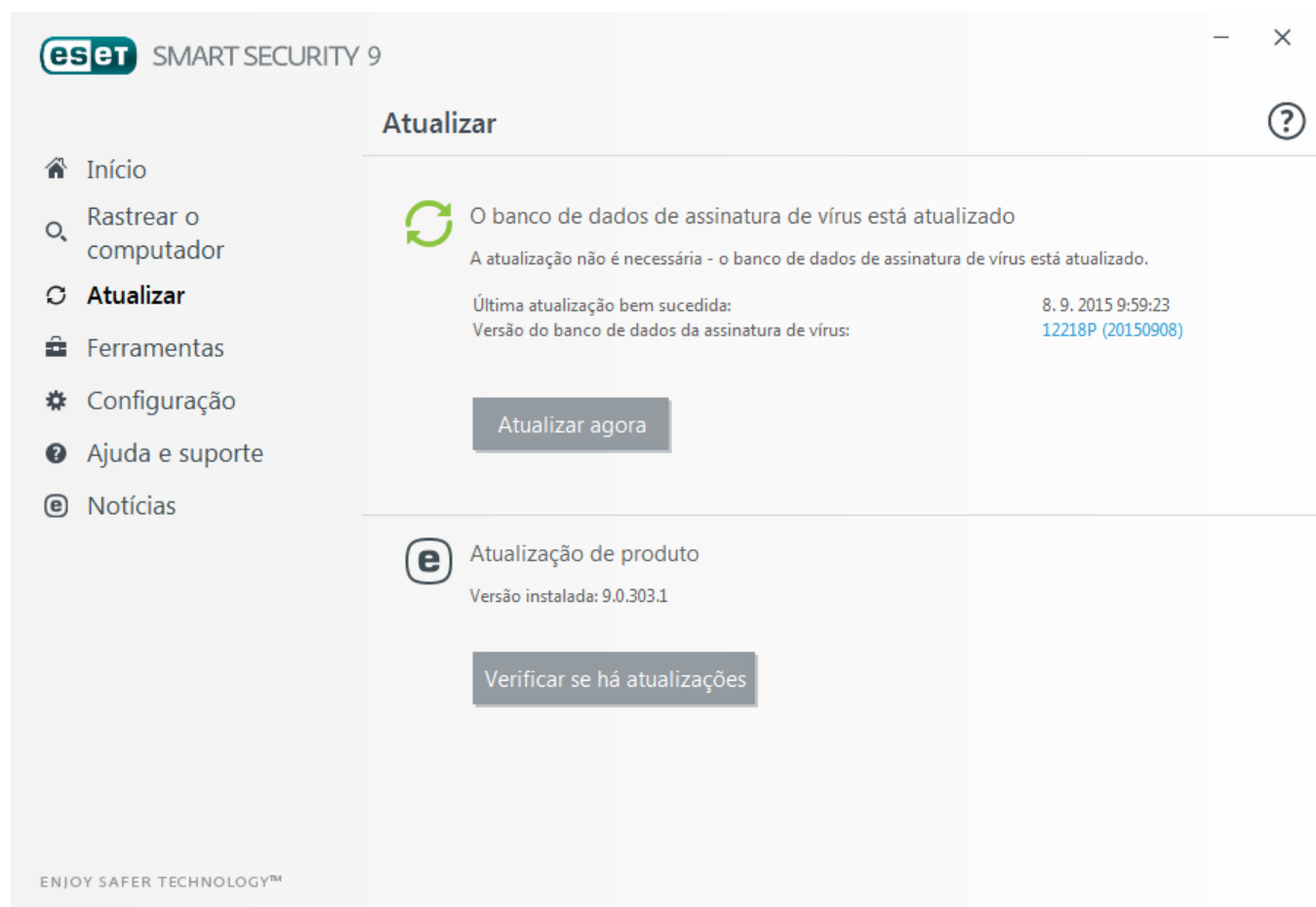
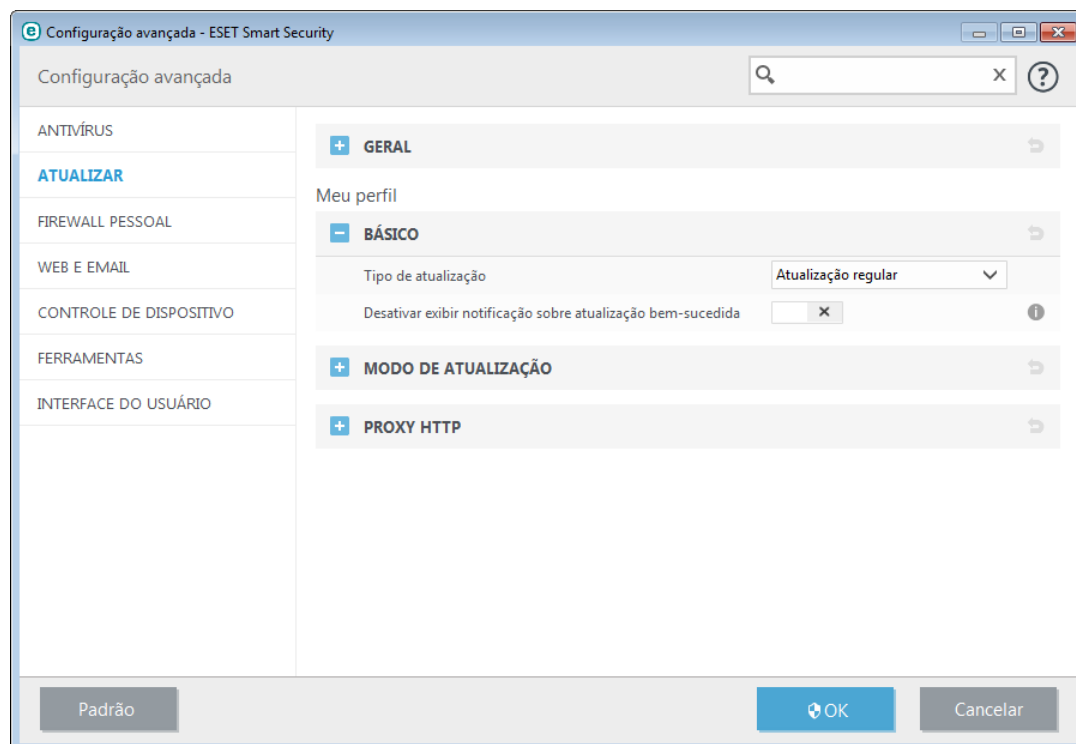
dispositivo como perdido) pode não ser criada no seu computador. É possível criar uma Conta fantasma usando o recurso Otimização na interface web do ESET Antifurto.

- **Modo de jogos ativado** - ativar o modo de jogos é um risco de segurança em potencial. Ativar este recurso desativa todas as janelas de pop-up e interrompe qualquer tarefa agendada.
- **Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação ao lado do relógio do sistema. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção ficará vermelho.

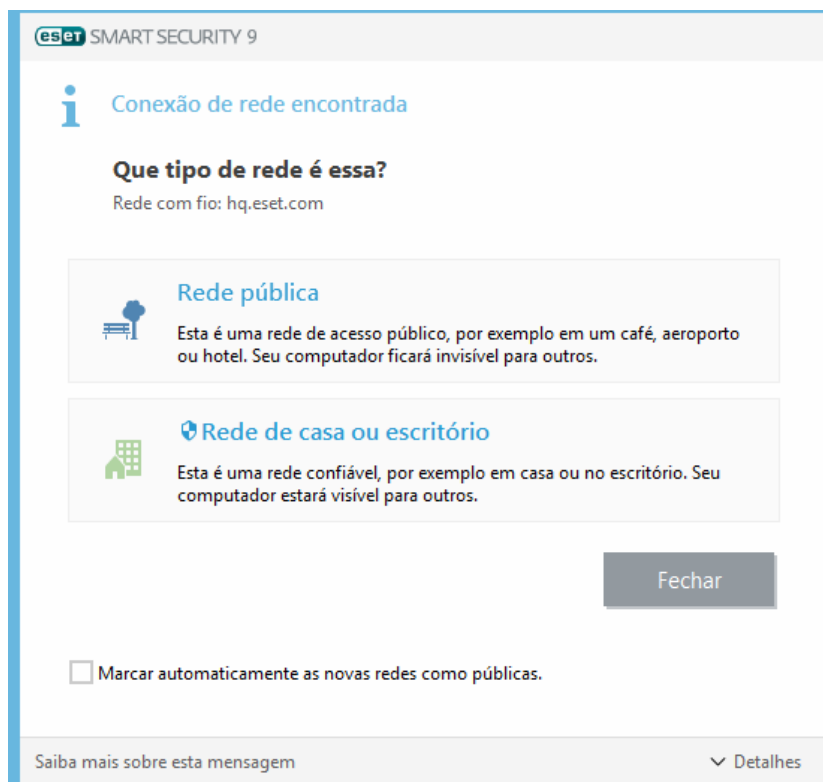
Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na Base de conhecimento da ESET. Se precisar de assistência, envie uma solicitação de suporte. O Atendimento ao Cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a encontrar uma solução.

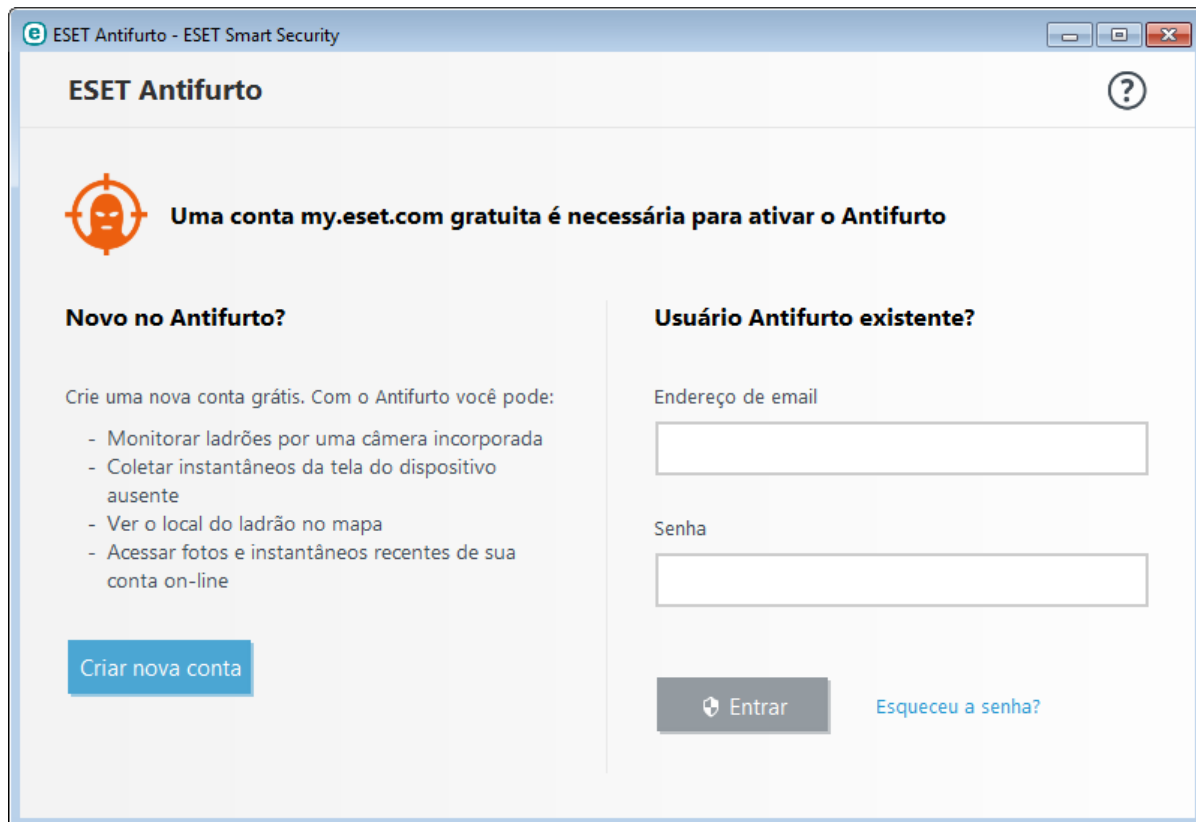
3.2 Atualizações

A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes na proteção completa do seu sistema contra códigos maliciosos. Dê atenção especial à sua configuração e operação. No menu principal, clique em **Atualizar** e em **Atualizar agora** para verificar se há uma atualização do banco de dados de assinatura de vírus.

Se o nome de usuário e a senha não foram fornecidos durante a ativação do ESET Smart Security, o sistema solicitará esses dados agora.

A janela Configuração avançada (no menu principal, clique em **Configuração** e depois em **Configuração avançada** ou pressione **F5** no teclado) contém opções de atualização adicionais. Para configurar opções avançadas de atualização como o modo de atualização, acesso ao servidor proxy e as conexões de rede, clique em uma guia particular na janela **Atualizar**.

3.3 Configuração de zona Confiável

É necessário configurar zonas confiáveis para proteger o computador em um ambiente de rede. É possível permitir que outros usuários acessem o seu computador configurando as zonas confiáveis e permitindo o compartilhamento. Clique em **Configuração** > **Proteção de rede** > **Redes conectadas** e clique no link abaixo da rede conectada. Uma janela exibirá as opções que permitem escolher o modo de proteção desejado do seu computador na rede.

A detecção de zona confiável ocorre após a instalação do ESET Smart Security e sempre que o seu computador se conectar a uma nova rede. Portanto, na maioria dos casos não há necessidade de definir as zonas confiáveis. Por padrão, uma janela da caixa de diálogo será exibida quando uma nova zona é detectada para configurar o nível de proteção dessa zona.

Aviso: Uma configuração incorreta da zona confiável pode representar um risco de segurança para o seu computador.

OBSERVAÇÃO: Por padrão, as estações de trabalho de uma Zona confiável têm acesso garantido a arquivos e impressoras compartilhados, a comunicação RPC de entrada é ativada e o compartilhamento da área de trabalho remota é disponibilizado.

Para mais detalhes sobre este recurso, leia o seguinte artigo na Base de conhecimento ESET:
Nova conexão de rede detectada no ESET Smart Security

3.4 Antifurto

Para proteger seu computador em caso de roubo ou perda, escolha uma das seguintes opções para registrar seu computador com o sistema ESET Antifurto.

1. Depois de uma ativação bem-sucedida, clique em **Ativar Antifurto** para ativar os recursos do ESET Antifurto para o computador que você acabou de registrar.

2. Se você vir a mensagem **ESET Antifurto está disponível**, no painel **Início** do ESET Smart Security, considere ativar esse recurso para seu computador. Clique em **Ativar ESET Antifurto** para registrar seu computador com o ESET Antifurto.

3. Na janela principal do programa, clique em **Configuração** > **Ferramentas de segurança.** Clique em ao lado de **ESET Antifurto** e siga as instruções na janela pop-up.

OBSERVAÇÃO: o ESET Antifurto não funciona no Microsoft Windows Home Server.

Para mais instruções sobre a associação de computador do ESET Antifurto veja Como adicionar um novo dispositivo.

3.5 Ferramentas do controle dos pais

Se você já tiver ativado o Controle dos pais no ESET Smart Security, também deverá configurar o Controle dos pais para contas de usuário desejadas, a fim de que o Controle dos pais funcione devidamente.

Quando os Controles dos pais estiverem ativos mas as contas de usuário não estiverem configuradas, a mensagem **O controle dos pais não está configurado** será exibida no painel **Início** da janela principal do programa. Clique em **Configurar regras agora** e consulte o capítulo Controle dos pais para obter instruções sobre como criar restrições específicas para seus filhos, a fim de protegê-los de material potencialmente ofensivo.

4. Trabalhando com o ESET Smart Security

as opções de configuração ESET Smart Security permitem que você ajuste os níveis de proteção do seu computador e da rede.

eset SMART SECURITY 9

Configuração

Início
Rastrear o computador
Atualizar
Ferramentas
Configuração
Ajuda e suporte
Notícias

Proteção do computador
Todos os recursos necessários para proteção do computador estão ativos.

Proteção de internet
Todos os recursos necessários para proteção de internet estão ativos.

Proteção de rede
Todos os recursos necessários para proteção de rede estão ativos.

Ferramentas de segurança
Ferramentas adicionais para proteger seu computador.

ENJOY SAFER TECHNOLOGY™
Importar/exportar configurações
Configuração avançada

O menu **Configurar** é dividido pelas seguintes seções:

Proteção do computador

Proteção de internet

Proteção de rede

Ferramentas de segurança

Clique em um componente para ajustar as configurações avançadas do módulo de proteção correspondente.

A configuração da proteção do Computador permite ativar ou desativar os seguintes componentes:

- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **HIPS** - O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo jogador** - ativa ou desativa o Modo jogador. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela principal será exibida em laranja após a ativação do Modo de jogos.

A configuração da proteção de Internet permite ativar ou desativar os seguintes componentes:

- **Proteção do acesso à web** - Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção de cliente de email** - monitora a comunicações recebida via protocolo POP3 e IMAP.
- **Proteção antispam** - Rastreia emails não solicitados (também conhecidos como spams).
- **Proteção antiphishing** - Filtra sites suspeitos de distribuir conteúdo com objetivo de manipular usuários para que enviem informações confidenciais.

A seção **Proteção de rede** permite ativar ou desativar o Firewall pessoal, Proteção contra ataques de rede (IDS) e Proteção contra botnet.

A configuração **Ferramentas de segurança** permite ajustar os módulos seguintes:

- Proteção de Atividade bancária e Pagamento
- Controle dos pais
- Antifurto

O Controle dos pais permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os pais podem proibir o acesso para mais de 40 categorias de site predefinidas e mais de 140 subcategorias.

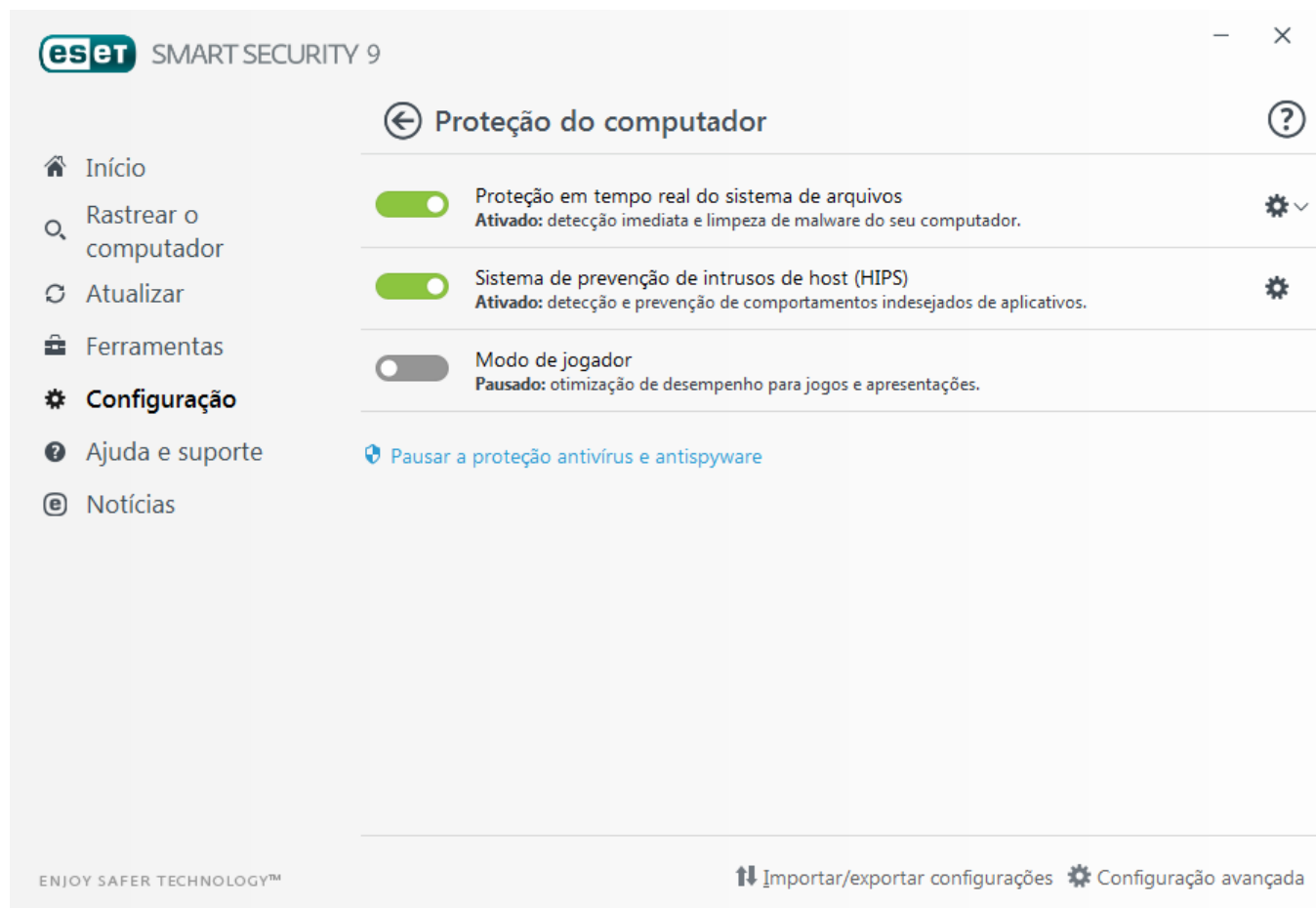
Para reativar a proteção do componente de segurança desativado, clique no controle deslizante para que ele mostre uma marca de verificação verde .

OBSERVAÇÃO: Ao desabilitar a proteção usando este método, todos os módulos com proteção desativada serão ativados depois da reinicialização do computador.

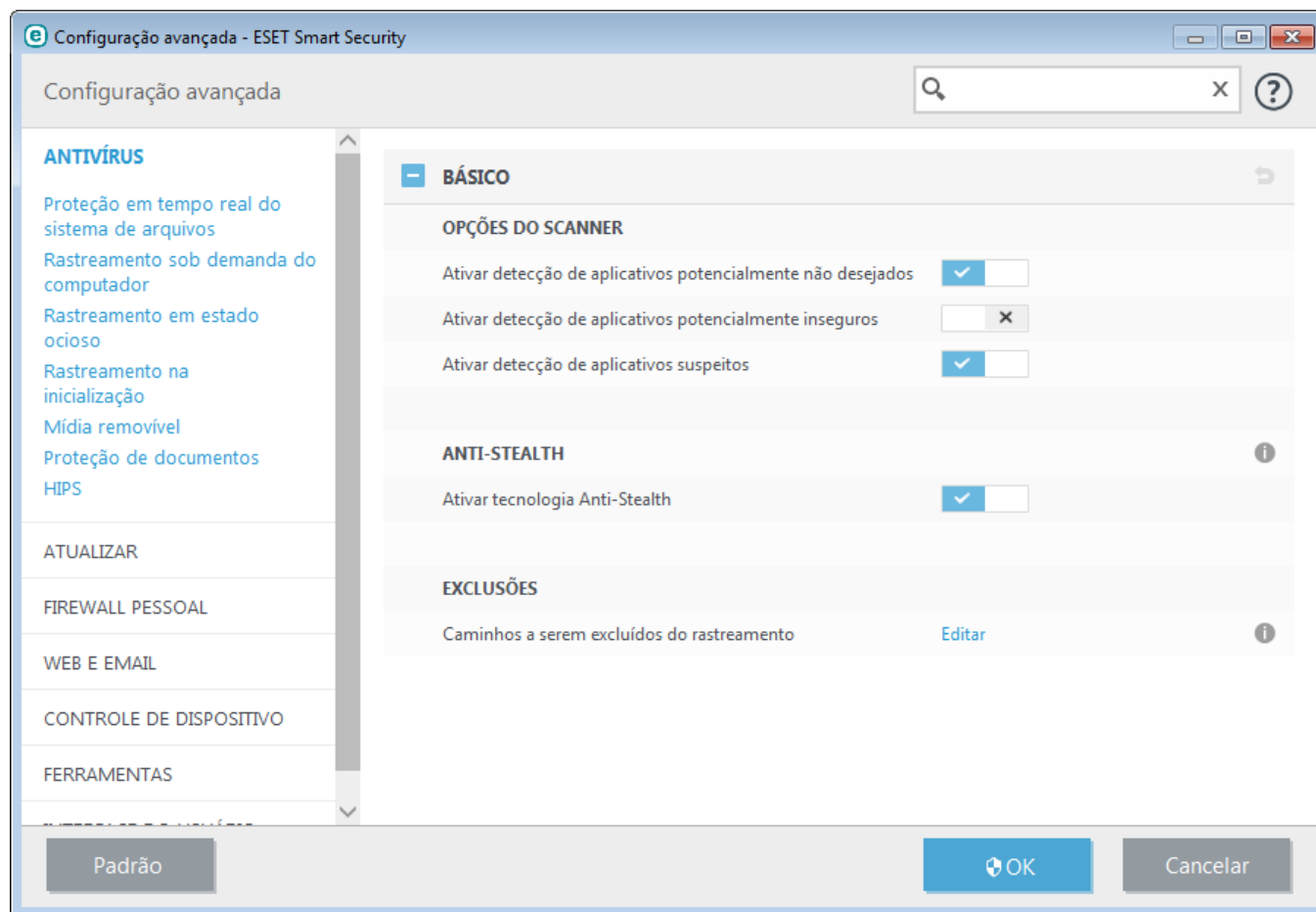
Existem opções adicionais disponíveis na parte inferior da janela de configuração. Use o link de **Configuração avançada** para configurar parâmetros mais detalhados para cada módulo. Use **Configurações importar/exportar** para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar seus parâmetros atuais em um arquivo de configuração.

4.1 Proteção do computador

Clique em Proteção do computador na janela de Configuração para uma visão geral de todos os módulos de proteção. Para desativar os módulos individuais temporariamente, clique em [toggle]. Observe que essa ação pode diminuir o nível de proteção do seu computador. Clique em [gear] ao lado de um módulo de proteção para acessar as configurações avançadas daquele módulo.

Clique em [gear] > **Editar exclusões** ao lado de **Proteção em tempo real do sistema de arquivos** para abrir a janela de configuração de Exclusão, que permite a exclusão de arquivos e pastas do rastreamento.

Pausar proteção antivírus e antispyware - Desativa todos os módulos de proteção antivírus e antispyware. Ao desativar a proteção uma janela será aberta, onde é possível determinar por quanto tempo a proteção estará desativada usando o menu suspenso **Intervalo de tempo**. Clique em **OK** para confirmar.

4.1.1 Antivírus

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la, primeiro bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

As **opções do scanner** para todos os módulos de proteção (p. ex., Proteção em tempo real do sistema de arquivos, Proteção do acesso à web, ...) permitem que você ative ou desative a detecção do seguinte:

- Os **Aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo.
  Leia mais sobre esses tipos de aplicativos no glossário.

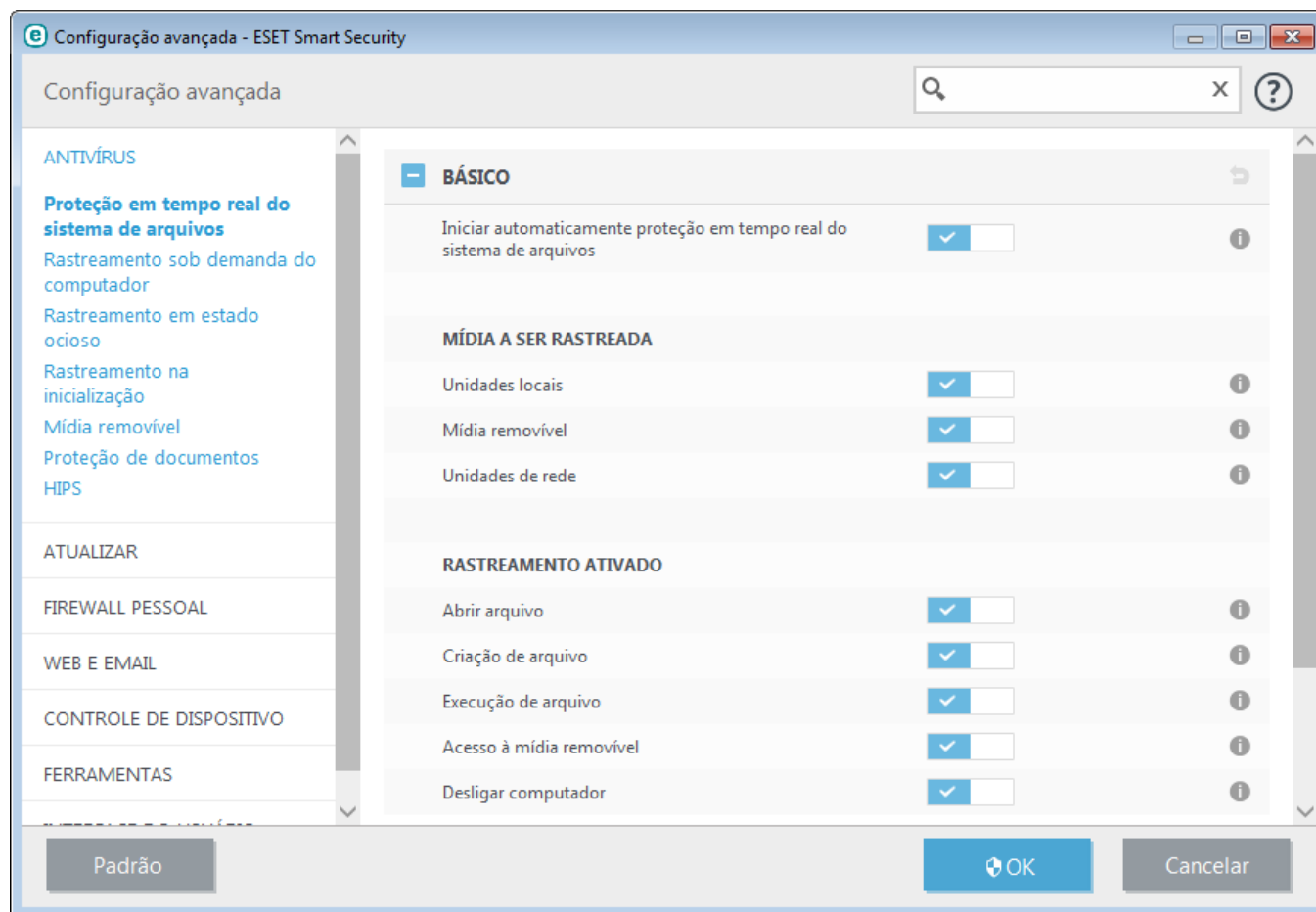
- **Aplicativos potencialmente inseguros** refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos. Exemplos de aplicativos potencialmente inseguros incluem ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.
  Leia mais sobre esses tipos de aplicativos no glossário.

- **Aplicativos suspeitos** incluem programas compactados com empacotadores ou protetores. Esses tipos de protetores são frequentemente explorados por autores de malware para impedir a detecção.

A tecnologia **Anti-Stealth** é um sistema sofisticado que fornece a detecção de programas nocivos, como os rootkits, que podem se auto ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

As **exclusões** permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Há situações em que você pode precisar excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação. Para excluir um objeto do rastreamento, consulte Exclusões.

4.1.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

Por padrão, a proteção em tempo real do sistema de arquivos é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outra proteção em tempo real), a proteção em tempo real pode ser desativada desmarcando **Iniciar proteção em tempo real do sistema de arquivos automaticamente** em **Configuração avançada**, em **Proteção em tempo real do sistema de arquivos** > **Básico**.

Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças:

Unidades locais - Controla todas as unidades de disco rígido do sistema.
Mídia removível - Controla CD/DVDs, armazenamento USB, dispositivos Bluetooth, etc.
Unidades de rede - Rastreia todas as unidades mapeadas.

Recomendamos que você use as configurações padrão e as modifique somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

Rastreamento ativado

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador:

- **Abertura de arquivo** - Ativa ou desativa o rastreamento quando arquivos estiverem abertos.
- **Criação de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem criados.
- **Execução de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem executados.
- **Acesso à mídia removível** - Ativa ou desativa o rastreamento disparado ao acessar mídia removível em particular com espaço de armazenamento.
- **Desligar computador** - Ativa ou desativa o rastreamento acionado por desligar o computador.

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense), a proteção em tempo real do sistema de arquivos pode ser configurada para tratar arquivos recém-criados de forma diferente dos arquivos existentes. Por exemplo, é possível configurar a Proteção em tempo real do sistema de arquivos para monitorar mais de perto os arquivos recém-criados.

Para garantir o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é controlado usando a **Otimização inteligente**. Se essa **Otimização inteligente** estiver desativada, todos os arquivos serão rastreados sempre que forem acessados. Para modificar essa configuração, pressione **F5** para abrir a Configuração avançada e expanda **Antivírus** > **Proteção em tempo real do sistema de arquivos**. Clique em **Parâmetro do ThreatSense**> **Outro** e marque ou desmarque **Ativar otimização inteligente**.

4.1.1.1.1 Parâmetros adicionais do ThreatSense

Parâmetros adicionais do ThreatSense para arquivos criados e modificados recentemente

A probabilidade de infecção em arquivos criados ou modificados recentemente é muito mais alta que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. O ESET Smart Security usa heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do banco de dados de assinatura de vírus com métodos de rastreamento baseados em assinatura. Além dos arquivos recém-criados, o rastreamento também é executado em **Arquivos de autoextração** (.sfx) e em **Empacotadores em tempo real** (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desmarque **Configurações padrão de rastreamento em arquivos compactados**.

Parâmetros adicionais do ThreatSense para arquivos executados

Heurística avançada na execução de arquivos - Por padrão, a Heurística avançada é utilizada quando os arquivos são executados. Quando ativada, é altamente recomendado manter a Otimização inteligente e o ESET LiveGrid® ativados para minimizar o impacto no desempenho do sistema.

Heurística avançada na execução de arquivos da mídia removível - A heurística avançada emula um código em um ambiente virtual e avalia seu comportamento antes do código poder ser executado a partir de uma mídia removível.

4.1.1.1.2 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar as configurações de nível de limpeza, clique em **Configuração do mecanismo ThreatSense** na seção **Proteção em tempo real do sistema de arquivos** e clique em **Limpeza**).

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza padrão - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

4.1.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos.

Após a instalação do ESET Smart Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique em ao lado de cada guia na janela (**Configuração avançada** > **Antivírus** > **Proteção do sistema de arquivos em tempo real**).

4.1.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo está disponível para download em http://www.eicar.org/download/eicar.com

OBSERVAÇÃO: Antes de realizar um rastreamento da proteção de tempo real, é preciso desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste.

4.1.1.1.5 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos problemas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** na janela principal do programa e clique em **Proteção do computador** > **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está desativada. Para garantir que esta opção está ativada, navegue para Configuração avançada (**F5**) e clique em **Antivírus** > **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se dois programas antivírus estiverem instalados ao mesmo tempo, eles podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema antes da instalação da ESET.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativado **Iniciar automaticamente proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Para ajuda na resolução deste problema, entre em contato com o Atendimento ao cliente da ESET.

4.1.1.2 Rastrear o computador

O rastreador sob demanda é uma parte importante da sua solução antivírus. Ele é usado para realizar rastreamentos nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema para detectar vírus que não tenham sido capturados pela Proteção em tempo real do sistema de arquivos quando foram gravados no disco. Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o banco de dados de vírus for obsoleto ou o arquivo não for detectado como vírus ao ser salvo no disco.

Há dois tipos de **Rastrear o computador** disponíveis. **Rastrear seu computador** rastreia rapidamente o sistema sem precisar especificar parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

 Rastrear seu computador

Rastrear seu computador permite que você inicie rapidamente um rastrear o computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem de Rastrear seu computador é que ele é fácil de operar e não requer configuração de rastreamento detalhada. Este rastreamento verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza.

 Rastreamento personalizado

O rastreamento personalizado permite especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

 Rastreamento de mídia removível

Semelhante ao Rastrear seu computador - inicie rapidamente um rastreamento de mídia removível (como CD/DVD/ USB) atualmente conectada ao computador. Isso pode ser útil quando você conectar uma unidade flash USB a um computador e quiser rastrear seu conteúdo quanto a malware e ameaças em potencial.

Esse tipo de rastreamento também pode ser iniciado clicando em **Rastreamento personalizado**, selecionando **Mídia removível** no menu suspenso **Alvos de rastreamento** e clicando em **Rastrear**.

 Repetir o último rastreamento

Permite iniciar rapidamente o rastreamento realizado anteriormente, usando as mesmas configurações com as quais foi executado antes.

Leia Progresso do rastreamento para obter mais informações sobre o processo de rastreamento.

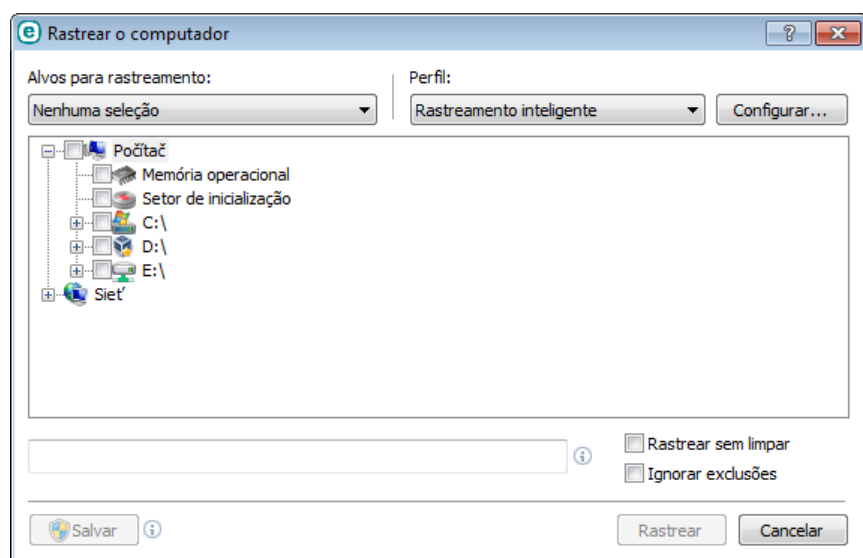
OBSERVAÇÃO: Recomendamos que execute um rastrear o computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Mais ferramentas** > **Agenda**. Como agendar um rastreamento semanal do computador?

4.1.1.2.1 Iniciador de rastreamento personalizado

Se desejar não verificar o espaço de disco inteiro, mas somente um alvo específico, você poderá usar a ferramenta Rastreamento personalizado clicando em **Rastrear o computador** > **Rastreamento personalizado** e selecionar uma opção no menu suspenso **Alvos de rastreamento** ou selecionar alvos específicos na estrutura de pasta (em árvore).

A janela Alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Nenhuma seleção** - Cancela todas as seleções.

Para navegar rapidamente até um alvo de rastreamento selecionado ou para adicionar diretamente um alvo desejado (pasta ou arquivo(s)), digite-o no campo em branco embaixo da lista de pastas. Isso só é possível se nenhum alvo tiver sido selecionado na estrutura em árvore e se o menu **Alvos de rastreamento** estiver definido como **Nenhuma seleção**.

Os itens infectados não são limpos automaticamente. O rastreamento sem limpar pode ser usado para obter uma visão geral do status de proteção atual. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**. As informações sobre o rastreamento serão salvas em um relatório de rastreamento.

Quando **Ignorar exclusões** está selecionado, os arquivos com extensões que foram excluídos do rastreamento anteriormente serão rastreados sem exceção.

Você pode escolher um perfil no menu suspenso **Perfil de rastreamento** para ser usado para rastreamento dos alvos escolhidos. O perfil padrão é **Rastrear seu computador**. Há mais dois perfis de rastreamento predefinidos intitulados **Rastreamento detalhado** e **Rastreamento do menu de contexto**. Estes perfis de rastreamento usam parâmetros ThreatSense diferentes. Clique em **Configuração...** para configurar em detalhes o perfil de rastreamento escolhido no menu Perfil de rastreamento. As opções disponíveis são descritas na seção **Outro** em ThreatSense parâmetros.

Clique em **Salvar** para salvar as alterações feitas na sua seleção de alvos, incluindo seleções feitas dentro da estrutura em árvore da pasta.

Clique em **Rastrear** para executar o rastreamento com os parâmetros personalizados definidos.

Rastrear como administrador permite que você execute o rastreamento usando a conta do administrador. Clique nessa opção se o usuário atual não tiver privilégios para acessar os arquivos apropriados para serem rastreados.

Observe que esse botão não estará disponível se o usuário atual não puder acionar operações de UAC como Administrador.

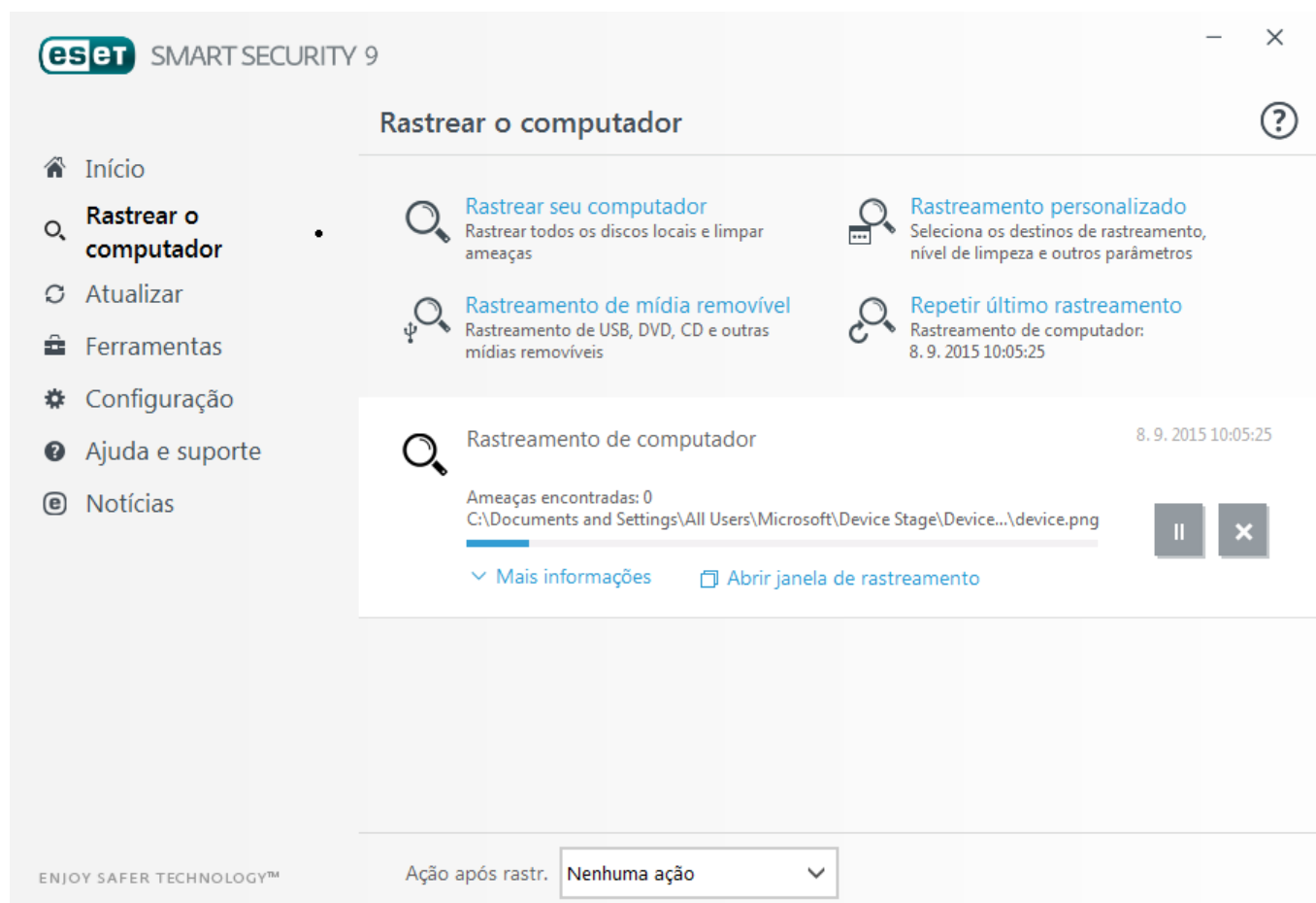
4.1.1.2.2 Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.

OBSERVAÇÃO: É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente *pagefile.sys* e determinados arquivos de log), não possam ser rastreados.

Progresso do rastreamento - A barra de progresso mostra o status de objetos já rastreados em relação aos objetos ainda aguardando para serem rastreados. O status de progresso do rastreamento é derivado do número total de objetos incluídos no rastreamento.
Destino - O nome do objeto rastreado no momento e sua localização.
Ameaças encontradas - Mostra o número total de arquivos rastreados, ameaças encontradas e ameaças limpas durante um rastreamento.
Pausa - Pausa um rastreamento.
Continuar - Essa opção torna-se visível quando o progresso do rastreamento é pausado. Clique em **Continuar** para dar continuidade ao rastreamento.
Parar - Termina o rastreamento.
Percorrer relatório de rastreamento - Se estiver ativado, o relatório de rastreamento rolará automaticamente para baixo à medida que novas entradas forem adicionadas para que as entradas mais recentes fiquem visíveis.

DICA:

Clique na lupa ou seta para mostrar detalhes sobre o rastreamento que está atualmente em execução.
Você pode executar outro rastreamento paralelo clicando em **Rastrear seu computador** ou **Rastreamento personalizado**.

Ação após o rastreamento - Aciona uma reinicialização ou desligamento agendado quando o rastreamento do computador for concluído. Assim que o rastreamento for concluído, uma janela de diálogo de confirmação do desligamento aparecerá e permanecerá aberta por 60 segundos.

4.1.1.2.3 Perfis de rastreamento

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Antivírus** > **Rastreamento sob demanda do computador** > **Básico** > **Lista de perfis**. A janela **Gerenciador de perfil** inclui o menu suspenso **Perfil selecionado** que lista perfis de rastreamento existentes e a opção de criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de **Rastrear seu computador** seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

4.1.1.3 Rastreamento na inicialização

Por padrão o rastreamento automático de arquivo na inicialização será executado na inicialização do sistema e durante a atualização do banco de dados de assinatura de vírus. Esse rastreamento depende das Tarefas e configurações da agenda.

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para alterar suas configurações, vá para **Ferramentas** > **Mais ferramentas** > **Agenda**, clique em **Verificação automática de arquivos de inicialização** e então em **Editar**. Na última etapa, a janela Rastreamento automático de arquivo na inicialização será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte Criação de novas tarefas.

4.1.1.3.1 Rastreamento de arquivos em execução durante inicialização do sistema

Ao criar uma tarefa agendada de Rastreamento de arquivo na inicialização do sistema, você tem várias opções para ajustar os seguintes parâmetros:

O menu suspenso **Arquivos usados comumente** especifica a profundidade do rastreamento da execução de arquivos na inicialização do sistema. Os arquivos são organizados em ordem decrescente de acordo com os seguintes critérios:

- **Todos os arquivos registrados** (mais arquivos rastreados)
- **Arquivos usados raramente**
- **Arquivos usados comumente**
- **Arquivos usados com frequência**
- **Somente os arquivos mais frequentemente usados** (últimos arquivos rastreados)

Dois grupos específicos também estão inclusos:

- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que podem ser acessados sem que o usuário esteja conectado (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que podem ser acessados após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

As listas de arquivos a serem rastreados estão fixas para cada grupo anteriormente.

Prioridade do rastreamento - O nível de prioridade usado para determinar quando um rastreamento iniciará:

- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Baixa** - em uma carga baixa do sistema,
- **Normal** - em uma carga média do sistema.

4.1.1.4 Rastreamento em estado ocioso

Você pode ativar o scanner em estado ocioso em **Configuração avançada** em **Antivírus** > **Rastreamento em estado ocioso** > **Básico**. Defina a opção ao lado de **Ativar rastreamento em estado ocioso** como **Ativado** para ativar esse recurso. Quando o computador estiver em estado ocioso, um rastreamento sem segundo plano do computador será realizado em todas as unidades locais. Veja Acionadores de detecção de estado ocioso para uma lista completa de condições que devem ser cumpridas para acionar o rastreamento de estado ocioso.

Por padrão, o rastreamento de estado ocioso não será executado quando o computador estiver fazendo uso de bateria. Você pode substituir essa configuração ativando a chave ao lado de **Executar mesmo se o computador estiver na bateria** na Configuração avançada.

Ative a opção **Ativar registro em relatório** na **Configuração avançada** > **Ferramentas** > **ESET LiveGrid®** para registrar uma saída de rastreamento do computador na seção Relatórios (a partir da janela principal do programa, clique em **Ferramentas** > **Relatórios** e selecione **Rastreamento do computador** a partir do menu suspenso **Relatório**).

A detecção em estado ocioso será executada quando o computador estiver em um dos seguintes estados:

- Proteção de tela
- Computador bloqueado
- Logoff de usuário

Clique na Configuração de parâmetros do mecanismo ThreatSense para modificar parâmetros de verificação (p. ex., métodos de detecção) para o scanner no estado ocioso.

4.1.1.5 Exclusões

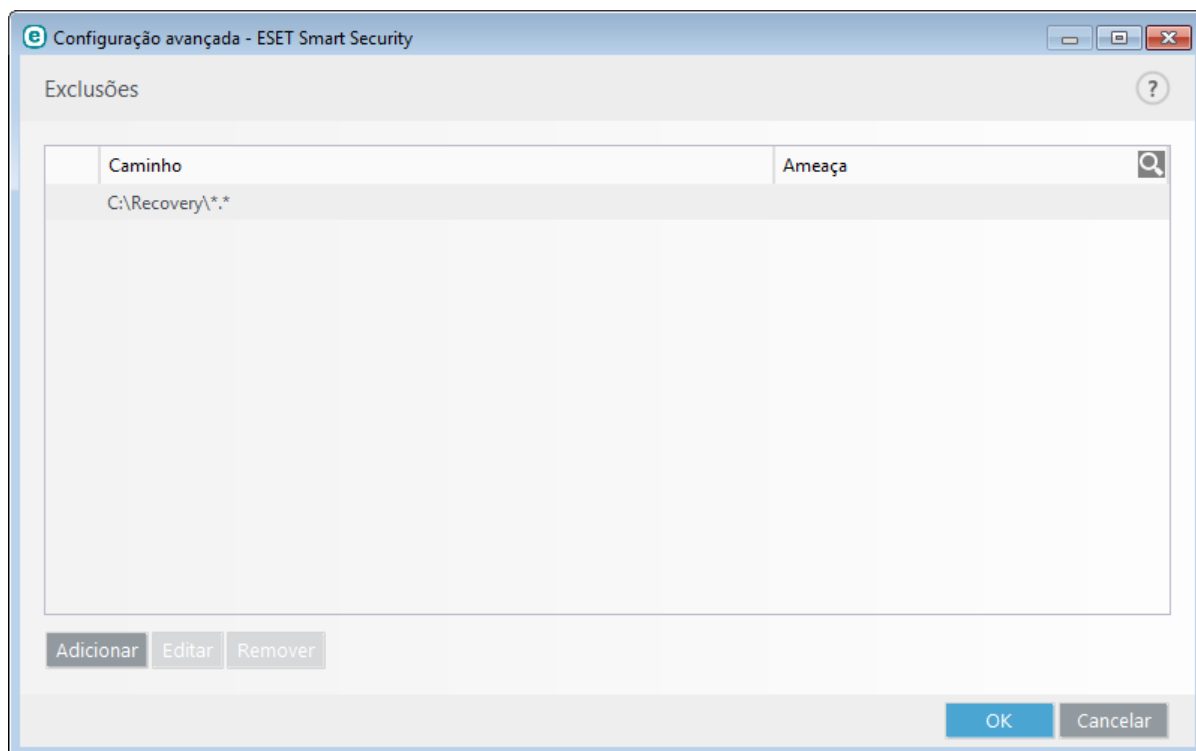
As exclusões permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Entretanto, existem situações em que você precisará excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação.

Para excluir um objeto do rastreamento:

1. Clique em **Adicionar**,
2. Digite o caminho para um objeto ou selecione-o na estrutura em árvore.

Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

Exemplos

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara “*.*”.
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara “*.doc”.
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, “D”), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).

OBSERVAÇÃO: uma ameaça em um arquivo não será detectada pelo módulo de proteção em tempo real do sistema de arquivos ou módulo de rastreamento do computador se um arquivo atender aos critérios para exclusão do rastreamento.

Colunas

Caminho - caminho para arquivos e pastas excluídos.

Ameaça - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, e não completamente. Se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus. Esse tipo de exclusão pode ser utilizado apenas para determinados tipos de infiltrações e pode ser criado na janela de alerta de ameaças que informa a infiltração (clique em **Mostrar opções avançadas** e selecione **Excluir da detecção**) ou clicando em **Ferramentas** > **Mais ferramentas** > **Quarentena** e depois clicando com o botão direito no arquivo de quarentena e selecionando **Restaurar e excluir da detecção** no menu de contexto.

Elementos de controle

Adicionar - exclui objetos da detecção.

Editar - permite que você edite as entradas selecionadas.

Remover - remove as entradas selecionadas.

4.1.1.6 Parâmetros ThreatSense

o ThreatSense é a tecnologia que consiste em muitos métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante a propagação inicial de uma nova ameaça. Ela utiliza uma combinação de análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

as opções de configuração do motor ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados,
- A combinação de diversos métodos de detecção,
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique em **parâmetros ThreatSense** na janela de Configuração avançada de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos,
- Rastreamento em estado ocioso,
- Rastreamento na inicialização,
- Proteção de documentos,
- Proteção do cliente de email,
- Proteção do acesso à web,
- Rastrear o computador.

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastrear o computador.

Objetos a serem rastreados

Esta seção permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

Memória operacional - Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização - Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

Arquivos de email - O programa oferece suporte às seguintes extensões: DBX (Outlook Express) e EML.

Arquivos compactados - O programa oferece suporte às seguintes extensões: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e muitas outras.

Arquivos compactados de auto extração - Os arquivos compactados de auto extração (SFX, Self-extracting archives) são arquivos compactados que não requerem programas especializados - arquivos compactados - para se descompactarem.

Empacotadores em tempo real - Depois da execução, os empacotadores em tempo real (ao contrário dos arquivos compactados padrão) fazem a descompactação na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o scanner é compatível com o reconhecimento de vários tipos adicionais de empacotadores graças à emulação do código.

Opções de rastreamento

Selecione os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

Heurística - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal vantagem dessa tecnologia é a capacidade de identificar software malicioso que não existia ou que não era conhecido pelo banco de dados das assinaturas de vírus anterior. A desvantagem é uma probabilidade (muito pequena) de alarmes falsos.

Heurística avançada/DNA/Assinaturas inteligentes - A heurística avançada consiste em um algoritmo de heurística exclusivo desenvolvido pela ESET, otimizado para detecção de worms e cavalos de troia no computador e escrito em linguagens de programação de alto nível. O uso de heurística avançada aumenta muito as capacidades de detecção de ameaças de produtos ESET. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

Um aplicativo potencialmente indesejado é um programa que contém adware, instala barras de ferramentas ou tem

outros objetivos pouco claros. Existem algumas situações em um usuário pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

Aviso - Ameaça em potencial encontrada

Quando um aplicativo potencialmente indesejado é detectado, você poderá decidir qual ação realizar:

1. **Limpar/Desconectar**: Esta opção encerra a ação e evita que uma possível ameaça entre no sistema.
2. **Ignorar**: Essa opção permite que a ameaça em potencial entre em seu sistema.
3. Para permitir que o aplicativo seja executado no seu computador no futuro sem interrupções, clique em **Opções avançadas** e selecione a caixa de seleção ao lado de **Excluir da detecção**.

Quando um aplicativo potencialmente indesejado é detectado e não é possível limpar, uma janela de notificação **O endereço foi bloqueado** será exibida no canto inferior direito da tela. Para mais informações sobre este evento vá para **Ferramentas** > **Mais ferramentas** > **Relatórios** > **Sites filtrados** no menu principal.

Aplicativos potencialmente indesejados - Configurações

Ao instalar seu produto ESET, é possível decidir se vai ativar a detecção de aplicativos potencialmente não desejados, conforme exibido abaixo:

Aplicativos potencialmente indesejados podem instalar adware, barras de ferramentas ou ter outros recursos de programa indesejados e inseguros.

Essas configurações podem ser modificadas nas suas configurações de programa a qualquer momento. Para ativar ou desativar a detecção de Aplicativos potencialmente indesejados, inseguros ou suspeitos, siga essas instruções:

1. Abra seu produto ESET. Como abrir meu produto ESET?
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Antivírus** e ative ou desative as opções **Ativar detecção de aplicativos potencialmente não desejados**, **Ativar detecção de aplicativos potencialmente inseguros** e **Ativar detecção de Ativar detecção de aplicativos suspeitos** de acordo com suas preferências. Confirme clicando em **OK**.

Aplicativos potencialmente indesejados - Wrapper de software

Um wrapper de software é um tipo especial de modificação de aplicativo que é usado por alguns sites de hospedagem de arquivos. É uma ferramenta de terceiros que instala o programa que você planejou baixar, mas adiciona outros software, como barras de ferramentas ou adware. O software adicional também pode fazer alterações na página inicial do seu navegador ou nas configurações de pesquisa. Além disso, sites de hospedagem de arquivos muitas vezes não notificam o fabricante do software ou receptor do download que modificações foram feitas e não permite que seja possível optar por não obter uma modificação com facilidade. Por esses motivos, a ESET classifica wrapper de software como um tipo de aplicativo potencialmente indesejado para permitir aos usuários aceitarem ou não seu download.

Consulte o seguinte artigo da Base de Conhecimento ESET para obter uma versão atualizada desta página de ajuda.

Aplicativos potencialmente inseguros - Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.

As configurações de limpeza determinam o comportamento do scanner enquanto limpa os arquivos infectados. Há três níveis de limpeza.

Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Outros

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento sob demanda do computador, as seguintes opções na seção **Outro** também estarão disponíveis:

Rastrear fluxos dados alternativos (ADS) - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade - Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

Registrar todos os objetos - Se essa opção estiver selecionada, o relatório mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados. Por exemplo, se uma infiltração for encontrada dentro de um arquivo compactado, o relatório também listará os arquivos limpos contidos dentro do arquivo compactado.

Ativar otimização inteligente - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Manter último registro de acesso - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Configurações do objeto

Tamanho máximo do objeto - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento. Valor padrão: *sem limite*.

Tempo máximo do rastreamento para objeto (segundos) - Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento. Valor padrão: *sem limite*.

Configuração de rastreamento em arquivos compactados

Nível de compactação de arquivos compactados - Especifica a profundidade máxima do rastreamento de arquivos compactados. Valor padrão: *10*.

Tamanho máximo do arquivo no arquivo compactado - Essa opção permite especificar o tamanho máximo de arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Valor padrão: *sem limite*.

OBSERVAÇÃO: Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

4.1.1.6.1 Limpeza

As configurações de limpeza determinam o comportamento do scanner enquanto limpa os arquivos infectados. Há três níveis de limpeza.

4.1.1.6.2 Extensões de arquivo excluídas do rastreamento

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando certas extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

Com os botões **Adicionar** e **Remover**, você pode autorizar ou proibir o rastreamento de extensões de arquivos específicas. Para adicionar uma nova extensão à lista, clique em **Adicionar**, digite a extensão no campo em branco e clique em **OK**. Quando você selecionar **Inserir valores múltiplos**, você poderá adicionar várias extensões de arquivos delimitadas por linhas, vírgulas ou ponto e vírgulas. Quando a seleção múltipla estiver ativada, extensões serão mostradas na lista. Selecione uma extensão na lista e clique em **Remover** para excluir essa extensão da lista. Se você quiser editar uma extensão selecionada, clique em **Editar**.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco representa qualquer string de caracteres e o ponto de interrogação representa qualquer símbolo.

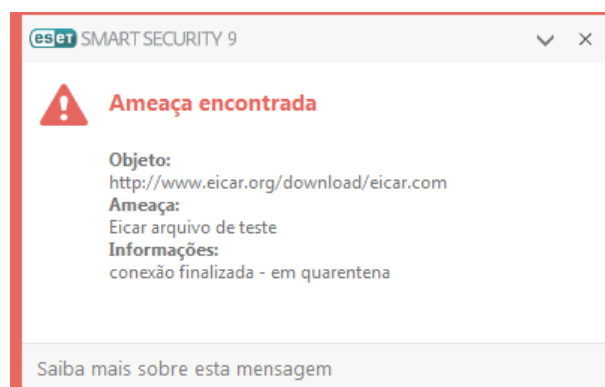
4.1.1.7 Uma infiltração foi detectada

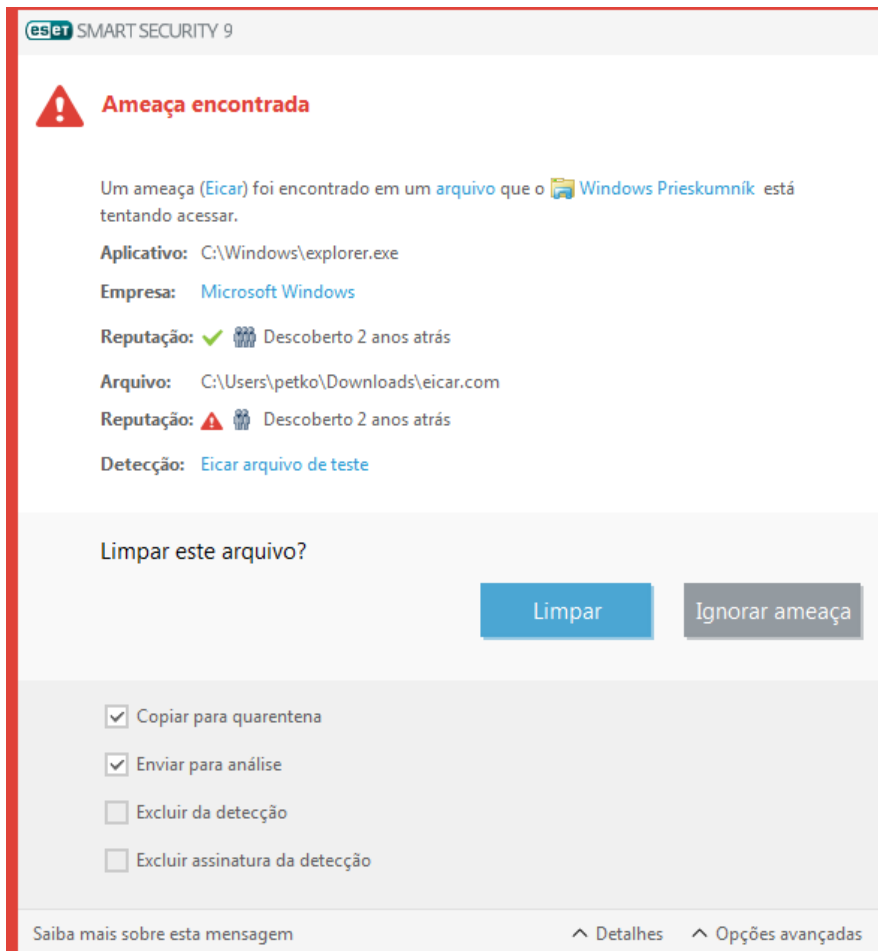
As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como páginas da web, pastas compartilhadas, via email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET Smart Security, as infiltrações podem ser detectadas usando:

- Proteção em tempo real do sistema de arquivos
- Proteção do acesso à Web
- Proteção do cliente de email
- Rastreamento sob demanda do computador

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a Quarentena ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para obter mais informações sobre níveis de limpeza e de comportamento, consulte Limpeza.

Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.

Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Várias ameaças

Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o nível de limpeza estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione as ações adequadas para esses arquivos. Selecione ações para os arquivos (as ações são definidas individualmente para cada arquivo na lista) e clique em **Fim**.

Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza ativado um arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Smart Security e clique em Rastrear o computador.
- Clique em **Rastrear seu computador** (para obter mais informações, consulte Rastreamento do computador)
- Após a conclusão do rastreamento, revise o log para obter informações como o número de arquivos rastreados, infectados e limpos

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

4.1.1.8 Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. A proteção de documentos fornece uma camada de proteção além da proteção do sistema de arquivos em tempo real, bem como pode ser desativada para aprimorar o desempenho em sistemas não expostos a um alto volume de documentos do Microsoft Office.

Integrar ao sistema ativa o sistema de proteção. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Antivírus** > **Proteção de documentos** na janela de **Configuração avançada**.

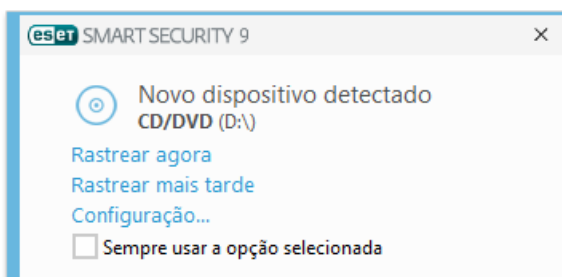
Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

4.1.2 Mídia removível

O ESET Smart Security fornece rastreamento automático de mídia removível (CD/DVD/USB/...). Este módulo permite que você rastreie uma mídia inserida. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

Ação a ser executada após inserção da mídia removível - Selecione a ação padrão que será desenvolvida quando um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Se a opção **Mostrar opções de rastreamento** for selecionada, será exibida uma notificação que lhe permite selecionar a ação desejada:

- **Não rastrear** - Nenhuma ação será executada e a janela **Novo dispositivo detectado** será fechada.
- **Rastreamento automático de dispositivo** - Um rastreamento do computador sob demanda do dispositivo de mídia removível inserido será executado.
- **Mostrar opções de rastreamento** - Abre a seção de configuração da mídia removível.

Quando uma mídia removível for inserida, a caixa de diálogo a seguir será exibida:

Rastrear agora - Isto vai acionar o rastreamento da mídia removível.

Rastrear mais tarde - O rastreamento da mídia removível será adiado.

Configuração - Abre a Configuração avançada.

Sempre usar a opção selecionada - Quando estiver selecionado, a mesma ação será executada quando uma mídia removível for inserida outra vez.

Além disso, o ESET Smart Security tem o recurso de Controle de dispositivos, que permite que você defina regras de

utilização de dispositivos externos em um determinado computador. Acesse a seção Controle de dispositivos para obter mais detalhes sobre o controle de dispositivos.

4.1.3 Controle de dispositivos

O ESET Smart Security fornece controle automático de dispositivos (CD/DVD/USB/...). Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

Dispositivos externos compatíveis:

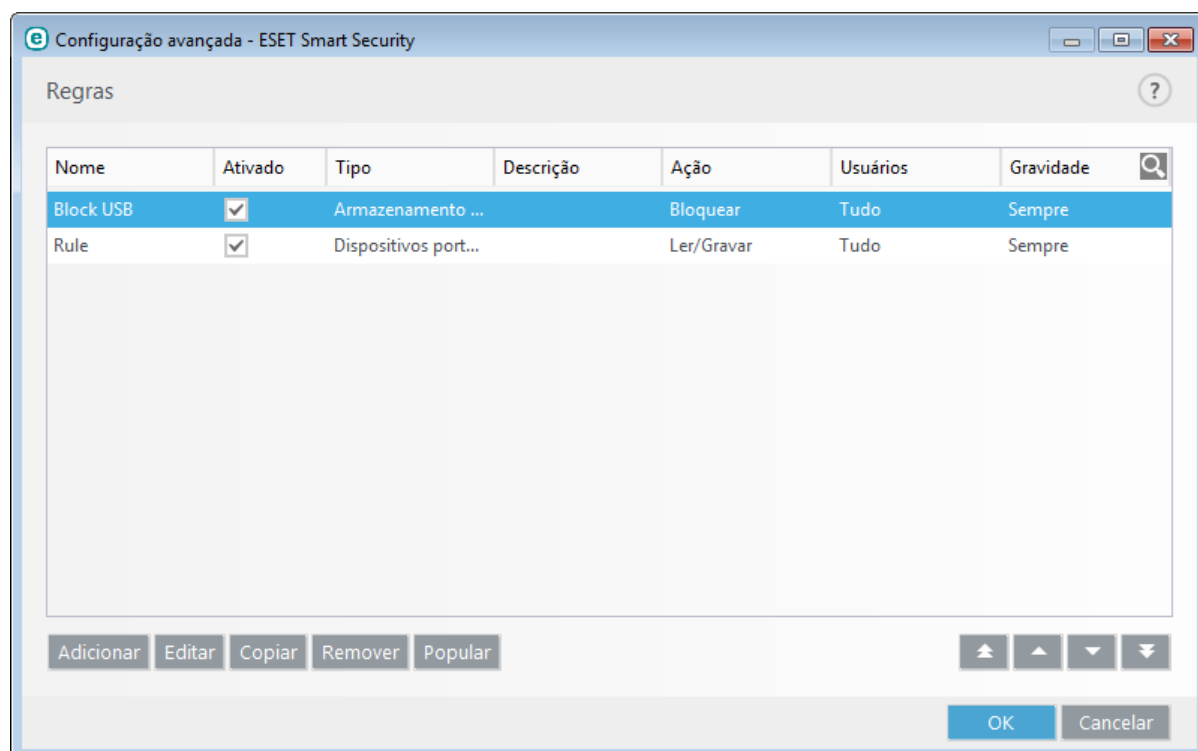
- Armazenamento em disco (HDD, disco removível USB)
- CD/DVD
- Impressora USB
- Armazenamento de FireWire
- Dispositivo Bluetooth
- Leitor de cartão inteligente
- Dispositivo de imagens
- Modem
- Porta LPT/COM
- Dispositivo portátil
- Todos os tipos de dispositivo

As opções de configuração do controle de dispositivos podem ser modificadas em **Configuração avançada** (F5) > **Controle de dispositivos**.

Marcar a opção ao lado de **Integrar no sistema** ativa o recurso de Controle de dispositivos no ESET Smart Security, você precisará reiniciar o computador para que as alterações tenham efeito. Quando o Controle de dispositivos estiver ativado, as **Regras** ficarão ativas, permitindo abrir a janela do Editor de regras.

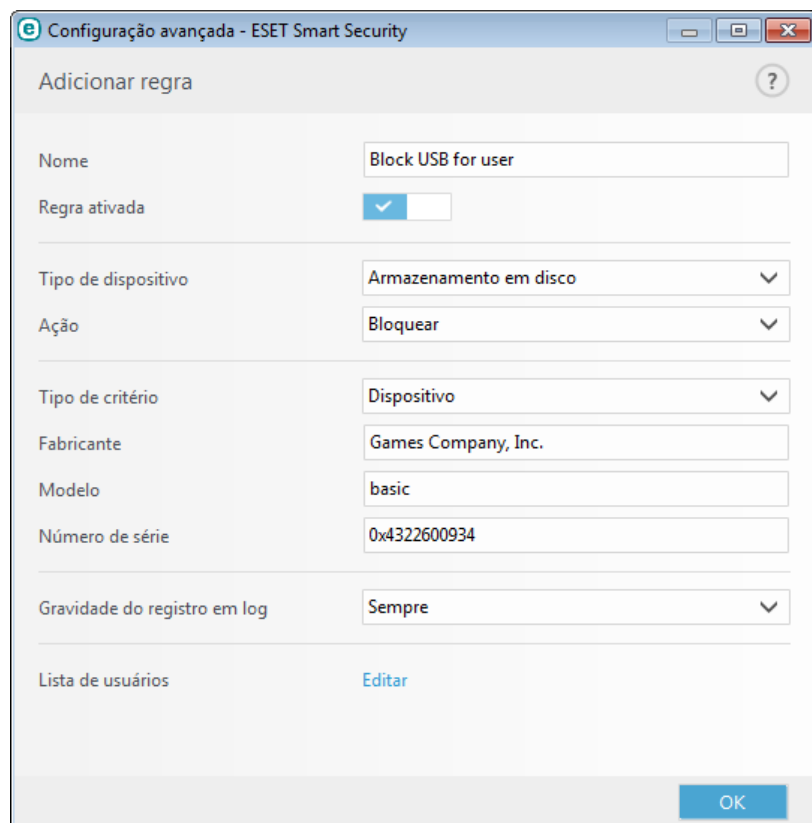
Se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida e o acesso ao dispositivo não será concedido.

4.1.3.1 Editor de regras do controle de dispositivos

A janela **Editor de regras do controle de dispositivos** mostra as regras existentes e permite que se controle de forma precisa os dispositivos externos que os usuários conectam ao computador.

Determinados dispositivos podem ser permitidos ou bloqueados por usuário ou grupo de usuários e com base em parâmetros de dispositivos adicionais que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de dispositivo externo, ação a ser realizada após conectar um dispositivo externo ao seu computador e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Copiar** para criar uma nova regra com opções predefinidas usadas para outra regra selecionada. As cadeias XML exibidas ao clicar em uma regra podem ser copiadas para a área de transferência para ajudar os administradores do sistema a exportarem/importarem esses dados e usá-los, por exemplo no ESET Remote Administrator.

Ao pressionar CTRL e clicar, é possível selecionar mais de uma regra e aplicar as ações, tais como exclui-las ou movê-las para cima e para baixo na lista, em todas as regras selecionadas. A caixa de seleção **Ativado** desativará ou ativará uma regra; isso pode ser útil caso não deseje excluir uma regra permanentemente se você pretende usá-la no futuro.

O controle é realizado por regras classificadas na ordem que determina sua prioridade, com regras de prioridade mais alta na parte superior.

As entradas de relatórios podem ser visualizadas a partir da janela principal do ESET Smart Security em **Ferramentas** > **Mais ferramentas** > **Relatórios**.

O relatório de controle de dispositivos registra todas as ocorrências nas quais o controle de dispositivos é acionado.

Clique em **Preencher** para preencher automaticamente os parâmetros do dispositivo de mídia removível para dispositivos conectados ao computador.

4.1.3.2 Adição de regras do controle de dispositivos

Uma Regra de controle de dispositivos define a ação a ser tomada quando um dispositivo que corresponde aos critérios da regra é conectado ao computador.

Insira uma descrição da regra no campo **Nome** para melhor identificação. Clique na opção ao lado de **Regra ativada** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Tipo de dispositivo

Escolha o tipo de dispositivo externo no menu suspenso (Armazenamento em disco/Dispositivo portátil/Bluetooth/FireWire/...). As informações sobre o tipo de dispositivo são coletadas do sistema operacional e podem ser visualizados no Gerenciador de dispositivos do sistema se um dispositivo estiver conectado ao computador. Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Leitores de cartões inteligentes abrangem todos os leitores de cartões inteligentes com um circuito integrado incorporado, como cartões SIM ou cartões de autenticação. Scanners e câmeras são exemplos de dispositivos de imagens. Como esses dispositivos oferecem apenas informações sobre suas ações e não oferecem informações sobre os usuários, eles só podem ser bloqueados de forma global.

Ação

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de uma das seguintes configurações de direitos:

- **Ler/Gravar** - Será permitido acesso total ao dispositivo.
- **Bloquear** - O acesso ao dispositivo será bloqueado.
- **Apenas leitura** - Será permitido acesso apenas para leitura ao dispositivo.
- **Alertar** - Cada vez que um dispositivo for conectado, o usuário será notificado se ele é permitido ou bloqueado, e um registro no relatório será feito. Dispositivos não são lembrados, uma notificação continuará a ser exibida com conexões subsequentes ao mesmo dispositivo.

Note que nem todas as ações (permissões) estão disponíveis para todos os tipos de dispositivos. Se for um dispositivo do tipo armazenamento, todas as quatro Ações estão disponíveis. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos, bloqueados ou alertados).

Tipo de critério - Selecione **Grupo do dispositivo** ou **Dispositivo.**

Outros parâmetros mostrados a seguir podem ser usados para ajustar as regras e adequá-las a dispositivos. Todos os parâmetros não fazem diferenciação entre letras maiúsculas e minúsculas:

- **Fabricante** - Filtragem por nome ou ID do fabricante.
- **Modelo** - O nome específico do dispositivo.
- **Número de série** - Os dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.

OBSERVAÇÃO: Se esses parâmetros estiverem indefinidos, a regra irá ignorar estes campos enquanto faz a correspondência. Os parâmetros de filtragem em todos os campos de texto não fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são aceitos.

DICA: Para ver informações sobre um dispositivo, crie uma regra para o tipo de dispositivos, conecte o dispositivo ao seu computador e, em seguida, verifique os detalhes do dispositivo no Relatório de controle de dispositivos.

Gravidade do registro em relatório

o ESET Smart Security salva eventos importantes em um arquivo de relatório, que pode ser exibido diretamente no menu principal. Clique em **Ferramentas** > **Mais ferramentas** > **Arquivos de relatório** e então selecione **Controle de dispositivos** no menu suspenso **Relatório**.

- **Sempre** - criar relatório de todos os eventos.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Aviso** - Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum registro será feito.

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à **Lista de usuários**:

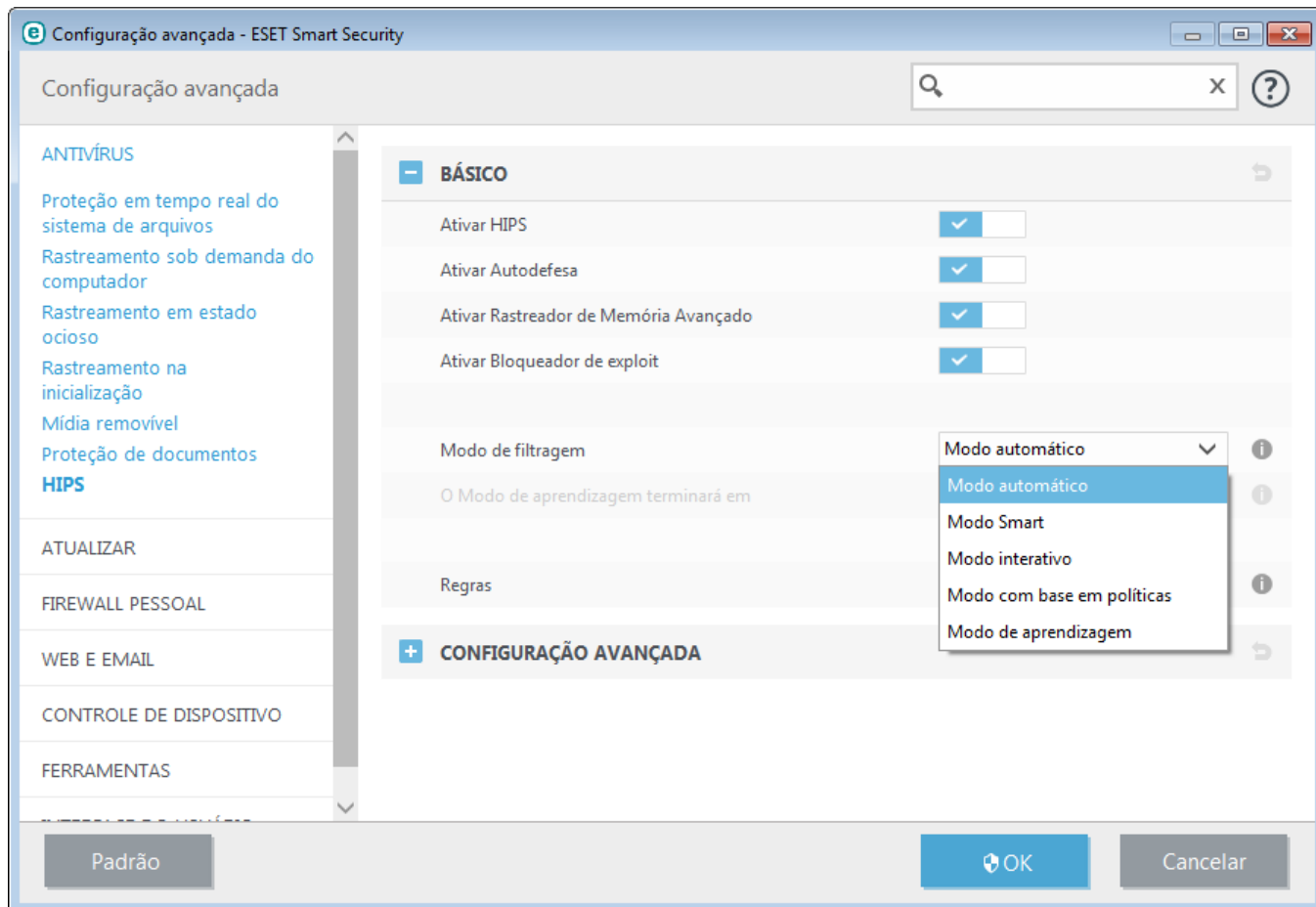
- **Adicionar** - Abre os **Tipos de objeto: Usuários ou Grupos** que permite selecionar os usuários desejados.
- **Remover** - Remove o usuário selecionado do filtro.

OBSERVAÇÃO: Todos os dispositivos podem ser filtrados por regras do usuário (por exemplo, dispositivos de criação de imagem não fornecem informações sobre usuários, apenas sobre ações).

4.1.4 Sistema de prevenção de intrusos de host (HIPS)

Apenas um usuário experiente deve fazer alterações nas configurações do HIPS. A configuração incorreta das configurações HIPS pode causar instabilidade no sistema.

O **Sistema de prevenção de intrusos de host** (HIPS) protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

As configurações HIPS podem ser encontradas em **Configuração avançada** (F5) > **Antivírus** > **HIPS** > **Básico**. O status do HIPS (ativado/desativado) é exibido na janela do programa principal do ESET Smart Security, em **Configuração** > **Proteção do computador**.

o ESET Smart Security usa uma tecnologia de **Autodefesa** incorporada para impedir que o software malicioso danifique ou desabilite a proteção antivírus e antispyware. Dessa forma, você poderá ter certeza que seu sistema está protegido o tempo todo. É preciso reiniciar o Windows para desativar o HIPS ou a Autodefesa.

O **Rastreamento de memória avançado** funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o scanner de memória avançado está ativado. Leia mais sobre esse tipo de proteção no glossário.

O **Bloqueio de exploit** é feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no glossário.

A filtragem pode ser executada em um de quatro modos:

Modo automático - As operações são ativadas, exceto aquelas bloqueadas por regras predefinidas que protegem o sistema.

Modo Inteligente - O usuário será notificado apenas sobre eventos muito suspeitos.

Modo interativo - O sistema solicitará que o usuário confirme as operações.

Modo com base em políticas - As operações são bloqueadas.

Modo de aprendizagem - As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no Editor de regras, mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Quando selecionar o Modo de aprendizagem do menu suspenso Modo de filtragem HIPS, a configuração **Modo de aprendizagem vai terminar em** ficará disponível. Selecione a duração pela qual você deseja se envolver no módulo de aprendizado, a duração máxima é de 14 dias. Quando a duração especificada tiver terminado, você será solicitado a editar as regras criadas pelo HIPS enquanto ele estava no modo de aprendizagem. Você também pode escolher um modo de filtragem diferente, ou adiar a decisão e continuar usando o modo de aprendizagem.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares às regras usadas no firewall pessoal. Clique em **Editar** para abrir a janela de gerenciamento de regras do HIPS. Aqui é

possível selecionar, criar, editar ou excluir regras.

No exemplo a seguir demonstraremos como restringir o comportamento indesejado de aplicativos:

1. Nomeie a regra e selecione **Bloquear** no menu suspenso **Ação**.
2. Ative a opção **Notificar usuário** para exibir uma notificação sempre que uma regra for aplicada.
3. Selecione pelo menos uma operação para a qual a regra será aplicada. Na janela **Aplicativos de origem**, selecione **Todos os aplicativos** no menu suspenso para aplicar sua nova regra a todos os aplicativos que tentarem realizar qualquer das operações de aplicativo nos aplicativos especificados.
4. Selecione **Alterar estado de outro aplicativo**(todas as operações são descritas na ajuda do produto, que pode ser acessada pressionando F1).
5. Selecione **Aplicativos específicos** no menu suspenso e **Adicione** um ou vários aplicativos que deseja proteger.
6. Clique em **Concluir** para salvar sua nova regra.

4.1.4.1 Configuração avançada

As opções a seguir são úteis para depurar e analisar o comportamento de um aplicativo:

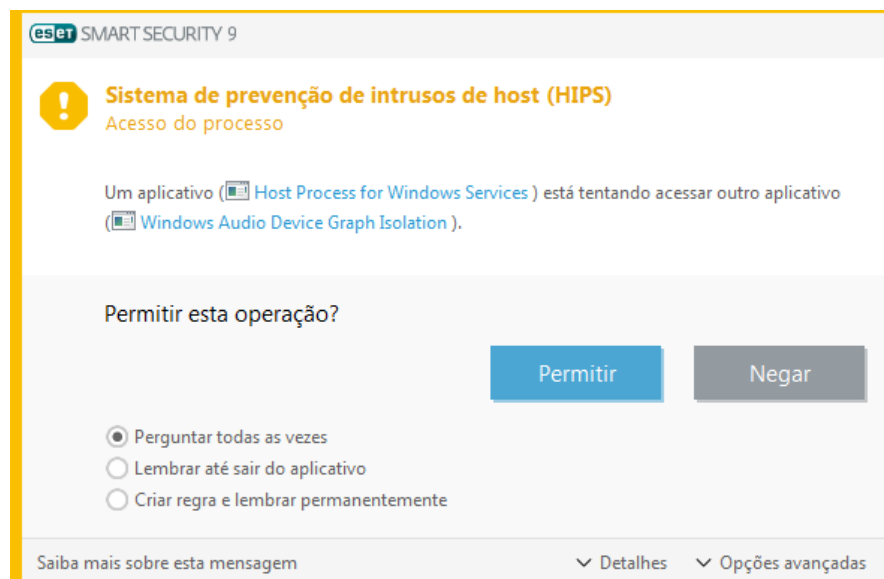
Drivers sempre com permissão para carregar - Os drivers selecionados sempre tem permissão para carregar, independentemente do modo de filtragem configurado, a menos que explicitamente bloqueado pela regra do usuário.

Registrar todas as operações bloqueadas - Todas as operações bloqueadas serão gravadas no log HIPS.

Notificar quando ocorrerem alterações nos aplicativos de Inicialização - Exibe uma notificação na área de trabalho toda vez que um aplicativo for adicionado ou removido da inicialização do sistema.

Consulte nosso artigo da Base de conhecimento para obter uma versão atualizada desta página de ajuda.

4.1.4.2 Janela interativa HIPS

Se a ação padrão para uma regra estiver definida como **Perguntar**, uma janela de diálogo será exibida sempre que a regra for acionada. Você pode optar por **Negar** ou **Permitir** a operação. Se você não definir uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

A janela da caixa de diálogo permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então definirá as condições nas quais permitir ou negar essa ação. Os parâmetros exatos podem ser definidos depois de clicar em **Detalhes**. As regras criadas como esta são consideradas iguais às regras criadas manualmente, portanto a regra criada a partir de uma janela de diálogo pode ser menos específica que a regra que acionou a janela de diálogo. Isso significa que após a criação dessa regra, a mesma operação pode acionar a mesma janela.

Lembrar até sair do aplicativo faz com que a ação (**Permitir/Negar**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

4.1.5 Modo jogador

O modo jogador é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Ao ativar esse recurso, todas as janelas pop-up são desativadas e a atividade da agenda será completamente interrompida. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

É possível ativar ou desativar o Modo jogador na janela principal do programa em **Configuração** > **Proteção do computador** clicando em ou ao lado de **Modo jogador**. Ativar automaticamente o modo de jogos é um risco de segurança em potencial, pois o ícone do status de proteção na barra de tarefas ficará laranja e exibirá um aviso. Esse aviso também pode ser visto na janela do programa principal, onde a opção **Modo de jogos ativado** será exibida em laranja.

O modo de jogos pode ser ativado na árvore de Configuração avançada (F5) expandindo **Computador**, clicando em **Modo de jogos** e marcando a caixa de seleção ao lado de **Ativar modo de jogos**.

Selecione **Ativar automaticamente o modo de jogos ao executar aplicativos em tela cheia** em Configuração avançada (F5) para que o modo de jogos seja iniciado sempre que você iniciar um aplicativo em tela cheia e seja interrompido automaticamente ao sair do aplicativo.

Selecione **Desativar o modo jogador automaticamente após** para definir o período de tempo após o qual o modo de jogador será desativado automaticamente.

OBSERVAÇÃO: se o firewall pessoal estiver no modo interativo e o modo de jogos for ativado, você pode ter dificuldades para conectar-se à Internet. Isso pode ser um problema se você iniciar um jogo on-line. Normalmente, você será solicitado a confirmar tal ação (se não houver regras de comunicação ou exceções definidas), mas a

interação com o usuário fará com que o modo de jogos seja desativado. Para permitir a comunicação, defina uma regra de comunicação para qualquer aplicativo que possa enfrentar esse problema, ou use um Modo de filtragem diferente no firewall pessoal. Tenha em mente que, se o modo de jogos estiver ativado e você acessar uma página da web ou um aplicativo que possa ser considerado um risco à segurança, eles poderão ser bloqueados sem nenhuma explicação ou aviso porque a interação com o usuário está desativada.

4.2 Proteção de internet

A configuração de Web e email pode ser encontrada no painel **Configuração** clicando em **Proteção de internet**. A partir daqui, você pode acessar configurações mais detalhadas do programa.

A conectividade com a Internet é um recurso padrão em computadores pessoais. Infelizmente, a Internet tornou-se o meio principal de distribuição de códigos maliciosos. Por esse motivo, é essencial refletir com atenção sobre as suas configurações de **Proteção do acesso à Web**.

Clique em ⚙ para abrir a web/email/antiphishing/antispam configurações de proteção em Configuração avançada.

Proteção do cliente de email fornece controle das comunicações por email recebida através dos protocolos POP3 e IMAP. Usando o plug-in do cliente de email, o ESET Smart Security permite controlar todas as comunicações enviadas e recebidas através do cliente de email (POP3, MAPI, IMAP, HTTP).

A **Proteção antispam** filtra mensagens de email não solicitadas.

Quando você clicar na roda de engrenagem ⚙ ao lado de **Proteção antispam**, as seguintes opções estão disponíveis:

Configurar... - Abre configurações avançadas para proteção antispam de cliente de email.

Lista de permissões/Lista de proibições/Lista de exceções de usuários - Abre uma janela de diálogo onde pode adicionar, editar ou excluir endereços de email considerados seguros ou não seguros. De acordo com as regras definidas aqui, o email desses endereços não será rastreado nem será tratado como spam. Clique em **Lista de exceções do usuário** para adicionar, editar ou excluir endereços de email que podem ser falsos e usados para o envio de spam. As mensagens de email de endereços relacionados na Lista de exceções serão sempre rastreadas quanto a spam.

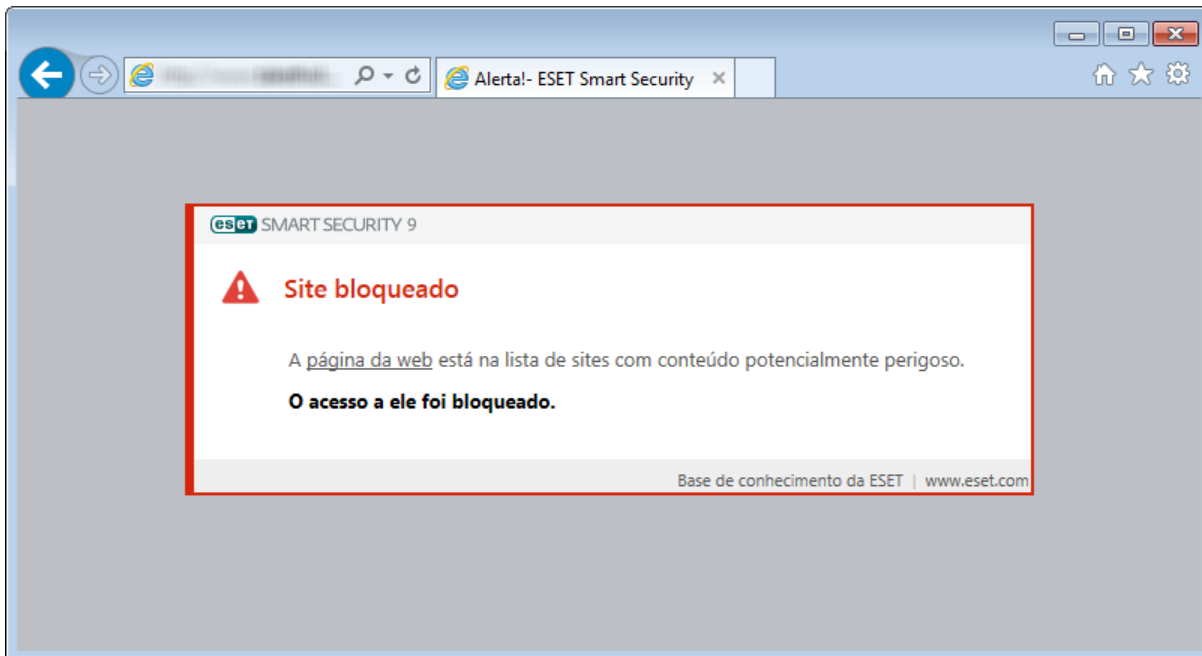
A **Proteção Antiphishing** permite bloquear páginas na web que são conhecidas como distribuindo conteúdo de roubo de identidade. Recomendamos que você deixe o Antiphishing ativado.

Você pode desativar o web/email/antiphishing/antispam temporariamente clicando em .

4.2.1 Proteção do acesso à Web

A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção de acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPS (comunicação criptografada).

O acesso à páginas da Web conhecidas como tendo conteúdo malicioso é bloqueado antes que o conteúdo seja baixado. Todas as outras páginas da Web serão rastreadas pelo mecanismo de rastreamento ThreatSense quando forem carregadas e bloqueadas se conteúdo malicioso for detectado. A proteção do acesso à Web oferece dois níveis de proteção, bloqueio por lista de proibições e bloqueio por conteúdo.

Recomendamos enfaticamente que a proteção de acesso à Web seja ativada. Essa opção pode ser acessada a partir da janela principal do ESET Smart Security localizada em **Configuração** > **Proteção de internet** > **Proteção do acesso à Web**.

As seguintes opções estão disponíveis em **Configuração avançada** (F5) > **Web e email** > **Proteção de acesso à Web**:

- **Protocolos da Web** - Permite que você configure o monitoramento para esses protocolos padrão, que são usados pela maioria dos navegadores de Internet.
- **Gerenciamento de endereços URL** - Permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.
- **parâmetros do ThreatSense** - Configuração avançada do rastreador de vírus - permite definir as configurações, como tipos de objetos para rastreamento (emails, arquivos, etc.), métodos de detecção para proteção do acesso à Web, etc.

4.2.1.1 Básico

Ativar proteção do acesso à Web - Quando desativado, a proteção do acesso à web e proteção antiphishing não serão garantidas.

OBSERVAÇÃO: Recomendamos que você deixe esta opção ativada.

4.2.1.2 Protocolos da web

Por padrão, o ESET Smart Security é configurado para monitorar o protocolo HTTP usado pela maioria dos navegadores de Internet.

Configuração do scanner HTTP

> No Windows Vista e versões posteriores, o tráfego HTTP é sempre monitorado em todas as portas para todos os aplicativos. No Windows XP, é possível modificar as **Portas utilizadas pelo protocolo HTTP** em **Configuração avançada** (F5) > **Web e email** > **Proteção do acesso à Web** > **Protocolos da Web**. O tráfego HTTP é monitorado nas portas especificadas para todos os aplicativos e em todas as portas para aplicativos marcados como Clientes Web e email.

Configuração do scanner HTTPS

> O ESET Smart Security também oferece suporte à verificação do protocolo HTTPS. A comunicação HTTPS utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Smart Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas definidas em **Portas usadas pelo protocolo HTTPS**, independentemente da versão do sistema operacional.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, vá para SSL/TLS na seção Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione a opção **Ativar filtragem de protocolo SSL/TLS**.

4.2.1.3 Gerenciamento de endereços URL

O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.

Sites na **Lista de endereços bloqueados** não estarão acessíveis, exceto se também forem incluídos na **Lista de endereços permitidos**. Sites na **Lista de endereços excluídos da verificação** não serão rastreados quanto a código malicioso quando acessados.

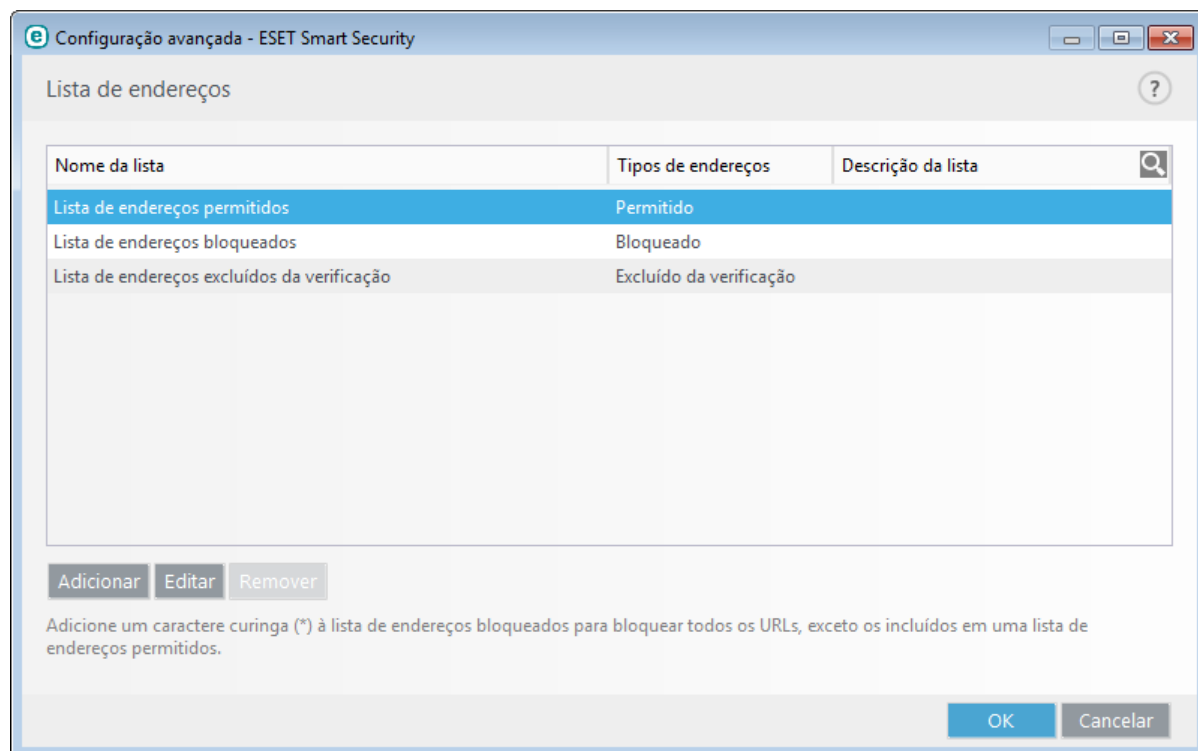
A opção **Ativar filtragem de protocolo SSL/TLS** deve ser selecionada se você quiser filtrar endereços HTTPS além de páginas HTTP. Caso contrário, somente os domínios de sites HTTPS que você tenha visitado serão adicionados, não a URL completa.

Se você adicionar um endereço URL à **Lista de endereços excluídos da filtragem**, o endereço será excluído do rastreamento. Você também poderá permitir ou bloquear determinados endereços, adicionando-os à **Lista de endereços permitidos** ou **Lista de endereços bloqueados**.

Se você quiser bloquear todos os endereços HTTP, exceto endereços presentes na **Lista de endereços permitidos** ativa, adicione * à **Lista de endereços bloqueados** ativa.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados em listas. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Consulte Adicionar endereço HTTP/máscara de domínio para saber como combinar com segurança um domínio completo, incluindo todos os subdomínios. Para ativar uma lista, selecione **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione **Notificar ao aplicar**.

DICA: O gerenciamento de endereços de URL também permite bloquear ou permitir a abertura de tipos de arquivo específicos durante a navegação na internet. Por exemplo, se não quiser que os arquivos executáveis sejam abertos,

selecione a lista de onde deseja bloquear esses arquivos no menu suspenso e insira a máscara "**.exe".

Elementos de controle

Adicionar - Crie uma nova lista além das predefinidas. Isso pode ser útil se você quiser dividir logicamente diferentes grupos de endereços. Por exemplo, uma lista de endereços bloqueados pode conter endereços de uma lista pública externa de proibições e uma segunda pode conter sua própria lista de proibições, facilitando a atualização da lista externa enquanto mantém a sua intacta.

Editar - Modifica listas existentes. Use isso para adicionar ou remover endereços.

Remover - Exclui as listas existentes. Disponível somente para listas criadas com **Adicionar**, não para as padrão.

4.2.2 Proteção do cliente de email

4.2.2.1 Clientes de email

A integração do ESET Smart Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Smart Security. Quando a integração for ativada, a barra de ferramentas do ESET Smart Security será inserida diretamente no cliente de email (a barra de ferramentas para versões mais recentes do Windows Live Mail não é inserida), permitindo proteção mais eficiente aos emails. As configurações de integração estão localizadas em **Configuração** > **Configuração avançada** > **Web e email** > **Proteção do cliente de email** > **Clientes de email**.

Integração com clientes de email

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

Ative a opção **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email (somente para MS Outlook). Essa situação pode ocorrer ao recuperar emails do Kerio Outlook Connector Store.

Email para ser rastreado

Email recebido - Alterna a verificação das mensagens recebidas.
Email enviado - Alterna a verificação das mensagens enviadas.
Email lido - Alterna a verificação das mensagens lidas.

Ação que será executada no email infectado

Nenhuma ação - Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.
Excluir email - O programa notificará o usuário sobre infiltrações e excluirá a mensagem.
Mover email para a pasta Itens excluídos - Os emails infectados serão movidos automaticamente para a pasta Itens excluídos.
Mover email para pasta - Os emails infectados serão movidos automaticamente para a pasta especificada.

Pasta - Especifique a pasta personalizada para a qual você deseja mover os emails infectados quando detectados.

Repetir o rastreamento após atualização - Alterna o rastreamento depois de uma atualização do banco de dados da assinatura de vírus.

Aceitar resultados de rastreamento de outros módulos - Se essa opção for selecionada, o módulo de proteção do email aceitará os resultados de rastreamento de outros módulos de proteção (rastreamento de aplicativos POP3, IMAP).

4.2.2.2 Protocolos de email

Os protocolos IMAP e POP3 são os protocolos mais amplamente utilizados para receber comunicação em um aplicativo cliente de email. O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de emails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de correio e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou excluída. O ESET Smart Security fornece proteção para estes protocolos, independentemente do cliente de email usado e sem precisar de uma nova configuração do cliente de email.

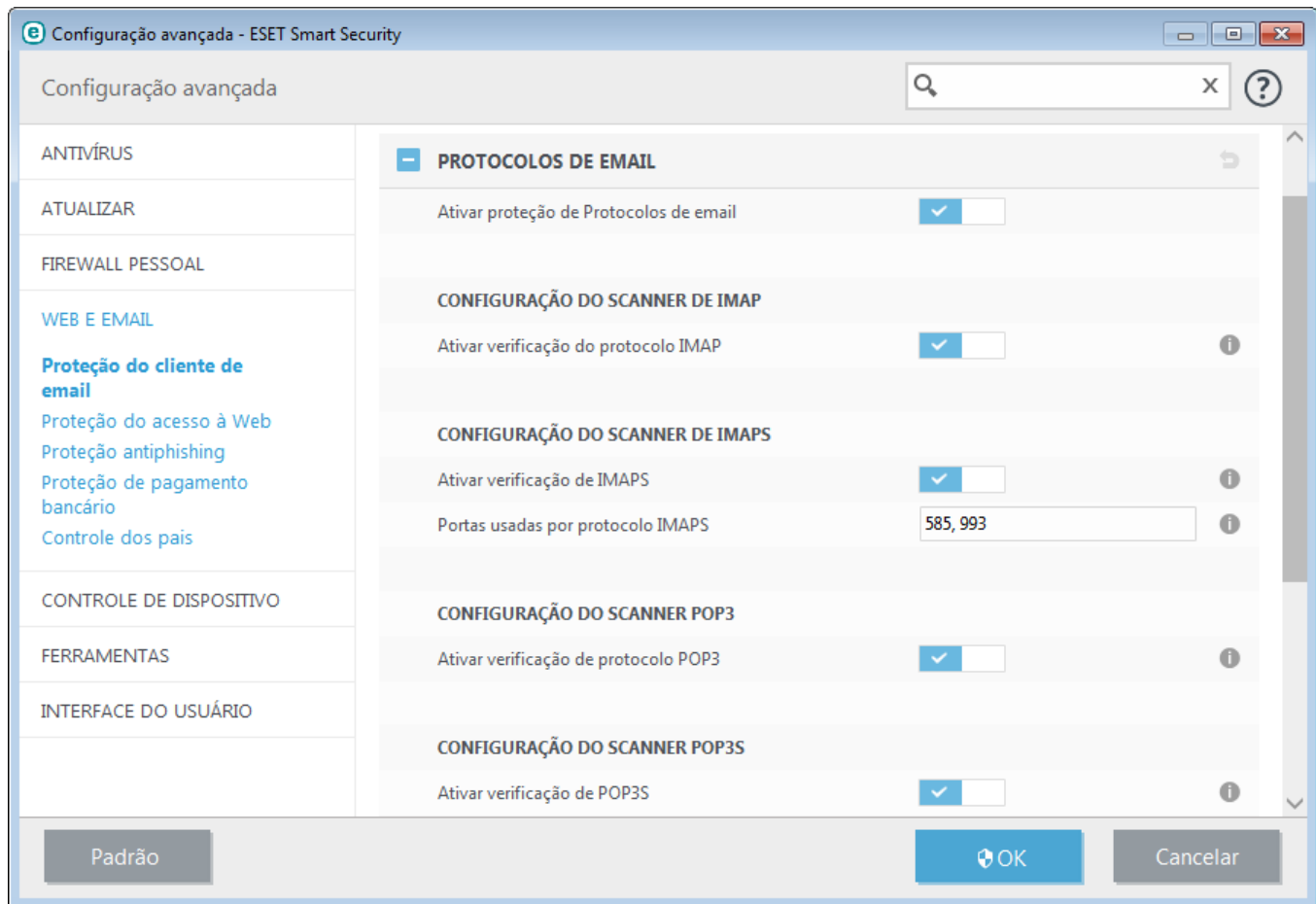
O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. O controle do protocolo IMAP é feito automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 143 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

Você pode configurar a verificação de protocolos IMAP/IMAPS e POP3/POP3S na Configuração avançada. Para acessar essa configuração, expanda **Web e email** > **Proteção do cliente de email** > **Protocolos de email**.

Ativar proteção de protocolos de email - Ativa a verificação de protocolos de email.

No Windows Vista e em versões posteriores, os protocolos IMAP e POP3 são automaticamente detectados e rastreados em todas as portas. No Windows XP, somente as **Portas usadas pelo protocolo IMAP/POP3** configuradas serão rastreadas para todos os aplicativos, assim como todas as portas serão rastreadas para aplicativos marcados como Clientes web e email.

O ESET Smart Security também é compatível com o rastreamento de protocolos IMAPS e POP3S, que utilizam um canal criptografado para transferir as informações entre servidor e cliente. O ESET Smart Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas definidas em **Portas usadas pelo protocolo IMAPS/POP3S**, independentemente da versão do sistema operacional.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, vá para SSL/TLS na seção Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione a opção **Ativar filtragem de protocolo SSL/TLS**.

4.2.2.3 Alertas e notificações

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Usando o plug-in para Microsoft Outlook e outros clientes de email, o ESET Smart Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado inclusos no mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** em **Web e email** > **Proteção do cliente de email** > **Alertas e notificações**.

Parâmetro ThreatSense - A configuração avançada do rastreamento de vírus permite configurar alvos do rastreamento, métodos de detecção, etc. Clique para exibir a janela de configuração do rastreamento de vírus detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. É possível selecionar **Acrescentar mensagem de marca nos emails recebidos e lidos**, **Acrescentar observação ao assunto de email infectado recebido e lido** ou **Acrescentar mensagens de marca a email enviado**. Esteja ciente que em algumas ocasiões mensagens de marca podem ser omitidas em mensagens HTML problemáticas ou se mensagem forem forjadas por malware. As mensagens de marca podem ser adicionadas a um email recebido e lido ou a um email enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Somente para email infectado** - Somente mensagens contendo software malicioso serão marcadas como rastreadas (padrão).
- **Para todos os emails rastreados** - o programa anexará mensagens a todos os emails rastreados.

Acrescentar observação ao assunto de email infectado enviado - Desative essa opção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples com base em assunto de email infectado (se compatível com o seu programa de email). Esse recurso aumenta o nível de

credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

Modelo adicionado ao assunto de email infectado - Edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado. Essa função substituirá o assunto da mensagem *"Olá"* com o prefixo *"[vírus]"* para o seguinte formato: *"[virus] Olá"*. A variável *%VIRUSNAME%* representa a ameaça detectada.

4.2.2.4 Integração com clientes de email

A integração do ESET Smart Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Smart Security. Quando a integração for ativada, a barra de ferramentas do ESET Smart Security será inserida diretamente no cliente de email, permitindo proteção mais eficiente aos emails. As configurações da integração estão disponíveis em **Configuração** > **Entrar na configuração avançada...** > **Web e email** > **Proteção do cliente de email** > **Integração com clientes de email**.

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Selecione a caixa de seleção próxima a **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao recuperar emails do Kerio Outlook Connector Store.

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

4.2.2.4.1 Configuração da proteção do cliente de email

O módulo de proteção do cliente de email suporta os seguintes clientes de email: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus.

4.2.2.5 Filtro POP3, POP3S

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET Smart Security fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado - a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os vários números das portas devem ser delimitados por vírgula.

A comunicação criptografada não será rastreada. Para ativar o rastreamento da comunicação criptografada e visualizar a configuração do scanner, vá para SSL/TLS na seção Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione a opção **Ativar filtragem de protocolo SSL/TLS**.

Nesta seção, é possível configurar a verificação dos protocolos POP3 e POP3S.

Ativar verificação do protocolo POP3 - Se estiver ativada, todo o tráfego por meio do POP3 será monitorado quanto a software malicioso.

Portas usadas pelo protocolo POP3 - Uma lista de portas utilizadas pelo protocolo POP3 (110 por padrão).

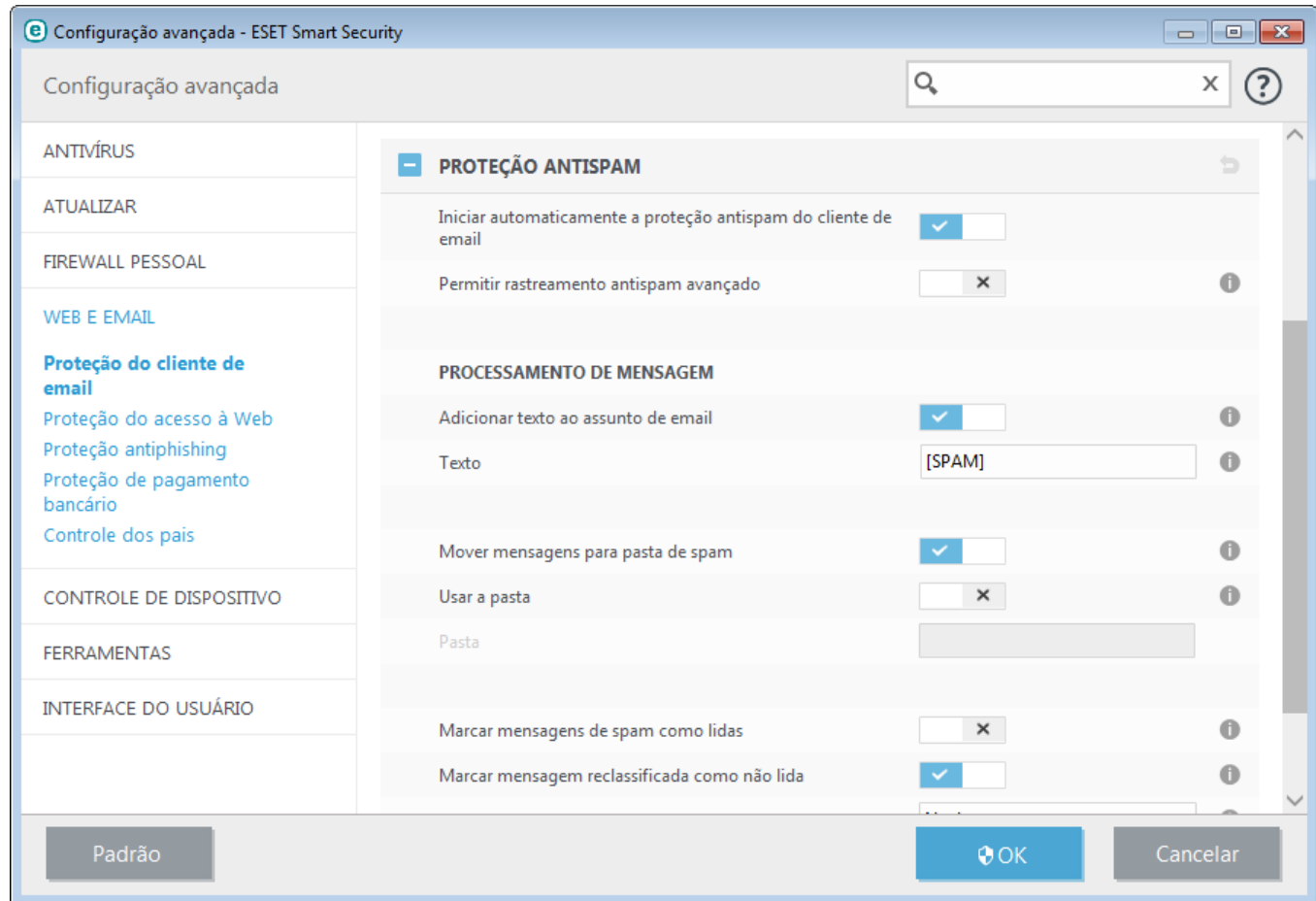
O ESET Smart Security oferece também suporte à verificação do protocolo POP3S. Esse tipo de comunicação utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Smart Security verifica as comunicações utilizando os métodos de criptografia SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte).

Não utilizar a verificação de POP3S - A comunicação criptografada não será verificada.

Utilizar a verificação de protocolo POP3S para as portas selecionadas - Selecione essa opção para permitir a verificação de POP3S apenas para as portas definidas em **Portas utilizadas pelo protocolo POP3S**.

Portas utilizadas pelo protocolo POP3S - Uma lista de portas POP3S a serem verificadas (por padrão, 995).

4.2.2.6 Proteção antispam

Os emails não solicitados, conhecidos como spams, estão entre os maiores problemas da comunicação eletrônica. Os spams representam até 80 por cento de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema. Combinando diversos princípios de segurança de email, o módulo Antispam fornece filtragem superior para manter a caixa de entrada limpa.

Um princípio importante para a detecção do spam é a capacidade de reconhecer emails não solicitados com base em endereços confiáveis predefinidos (lista de permissões) e em endereços de spam (lista de proibições). Todos os endereços de sua lista de contatos são automaticamente acrescentados à lista de permissões, bem como todos os demais endereços marcados pelo usuário como seguros.

O principal método usado para detectar spam é o rastreamento das propriedades da mensagem de email. As mensagens recebidas são verificadas quanto aos critérios Antispam básicos (definições da mensagem, heurísticas estatísticas, reconhecimento de algoritmos e outros métodos únicos) e o valor do índice resultante determina se uma mensagem é spam ou não.

Iniciar automaticamente a proteção antispam do cliente de email - Quando ativada, a proteção antispam será ativada automaticamente na inicialização do sistema.

Permitir rastreamento antispam avançado - Dados antispam adicionais serão baixados periodicamente, aumentando as capacidades antispam e produzindo melhores resultados.

A proteção antispam no ESET Smart Security permite definir diferentes parâmetros para trabalhar com as listas de emails. As opções são:

Processamento de mensagens

Adicionar texto ao assunto de email - Permite adicionar uma cadeia de caracteres de prefixo personalizado à linha

de assunto das mensagens classificadas como spam. O padrão é "[SPAM]".

Mover mensagens para pasta spam - Quando ativada, as mensagens de spam serão movidas para a pasta padrão de lixo eletrônico e as mensagens reclassificadas como não spam serão movidas para a caixa de entrada. Ao clicar com o botão direito em uma mensagem de email e selecionar ESET Smart Security no menu de contexto, é possível escolher das opções aplicáveis.

Usar a pasta - Esta opção move o spam para uma pasta definida pelo usuário.

Marcar mensagens de spam como lidas - Selecione isto para marcar automaticamente spam como lido. Isso o ajudará a concentrar sua atenção em mensagens "limpas".

Marcar mensagens reclassificadas como não lidas - As mensagens originariamente classificadas como spam, mas posteriormente marcadas como "limpas" serão exibidas como não lidas.

Registro em log da pontuação de spam - O mecanismo antispam do ESET Smart Security atribui uma pontuação de spam a cada mensagem rastreada. A mensagem será registrada no log de antispam (**ESET Smart Security** > **Ferramentas** > **Arquivos de log** > **Proteção antispam**).

- **Nenhum** - A pontuação do rastreamento antispam não será registrada.
- **Reclassificado e marcado como spam** - Selecione isto se desejar registrar uma pontuação de spam para mensagens marcadas como SPAM.
- **Todas** - Todas as mensagens serão registradas no relatório com a pontuação de spam.

OBSERVAÇÃO: Ao clicar em uma mensagem na pasta de email spam, é possível selecionar **Reclassificar mensagens selecionadas como NÃO spam** e a mensagem será movida para a caixa de entrada. Ao clicar em uma mensagem que você considera ser spam na caixa de entrada, selecione **Reclassificar mensagens como spam** e a mensagem será movida para a pasta de spam. Você pode selecionar várias mensagens e realizar a ação em todas elas ao mesmo tempo.

OBSERVAÇÃO: o ESET Smart Security é compatível com a proteção antispam para Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail.

4.2.3 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. A filtragem de protocolo funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. Para editar configurações criptografadas (SSL/TLS), acesse **Web e email** > **SSL/TLS**.

Ativar filtragem de conteúdo do protocolo de aplicativo - Essa opção pode ser usada para desativar a filtragem de protocolo. Observe que muitos componentes do ESET Smart Security (Proteção do acesso à Web, Proteção de protocolos de email, Antiphishing, Controle de Web) dependem disso e não funcionarão sem ele.

Aplicativos excluídos - Permite que você exclua aplicativos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Endereços IP excluídos - Permite que você exclua endereços remotos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Clientes Web e email - Opção usada somente em sistemas operacionais Windows XP; permite que você selecione aplicativos dos quais todo o tráfego será filtrado por filtragem de protocolo, independentemente das portas usadas.

4.2.3.1 Clientes web e de email

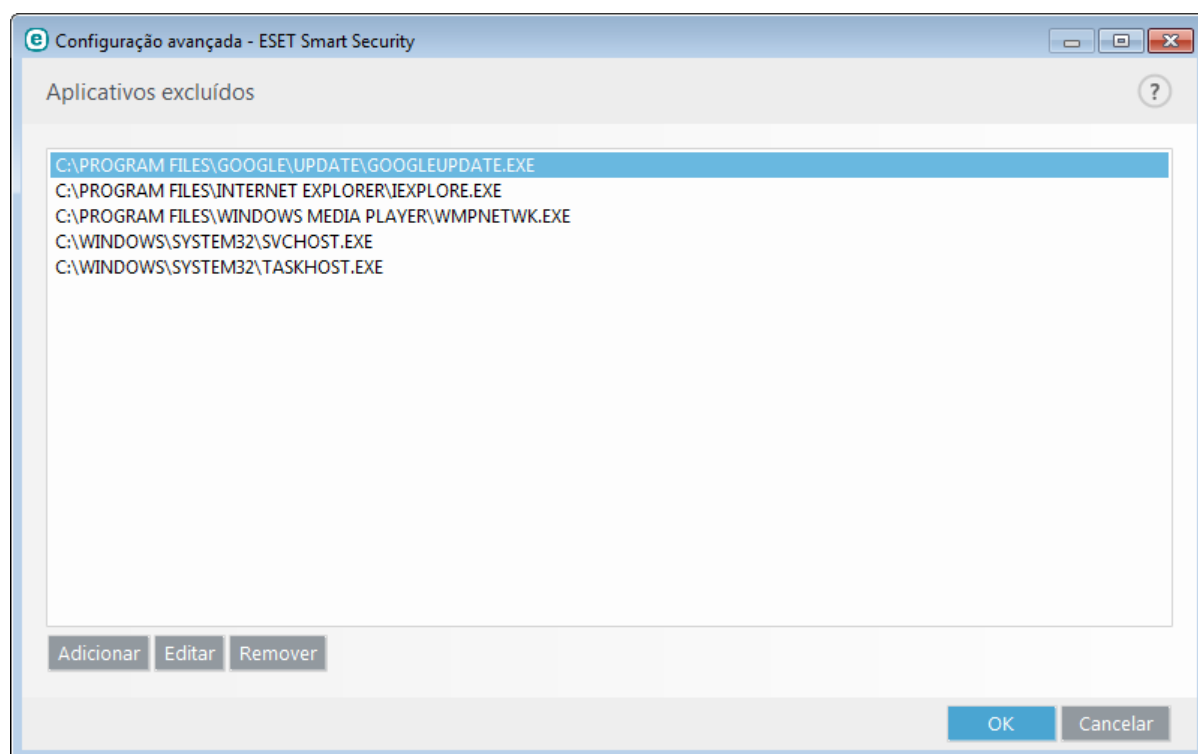
OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, a seção **Clientes web e de email** não está disponível.

Devido à enorme quantidade de códigos maliciosos circulando na Internet, a navegação segura é um aspecto muito importante na proteção do computador. As vulnerabilidades do navegador da Web e os links fraudulentos ajudam o código malicioso a entrar no sistema despercebido e é por isso que o ESET Smart Security se focaliza na segurança do navegador da web. Cada aplicativo que acessar a rede pode ser marcado como um navegador da Internet. A caixa de seleção possui dois estados:

- **Desmarcada** - A comunicação de aplicativos é filtrada apenas para as portas especificadas.
- **Marcada** - A comunicação é sempre filtrada (mesmo que uma porta diferente seja definida).

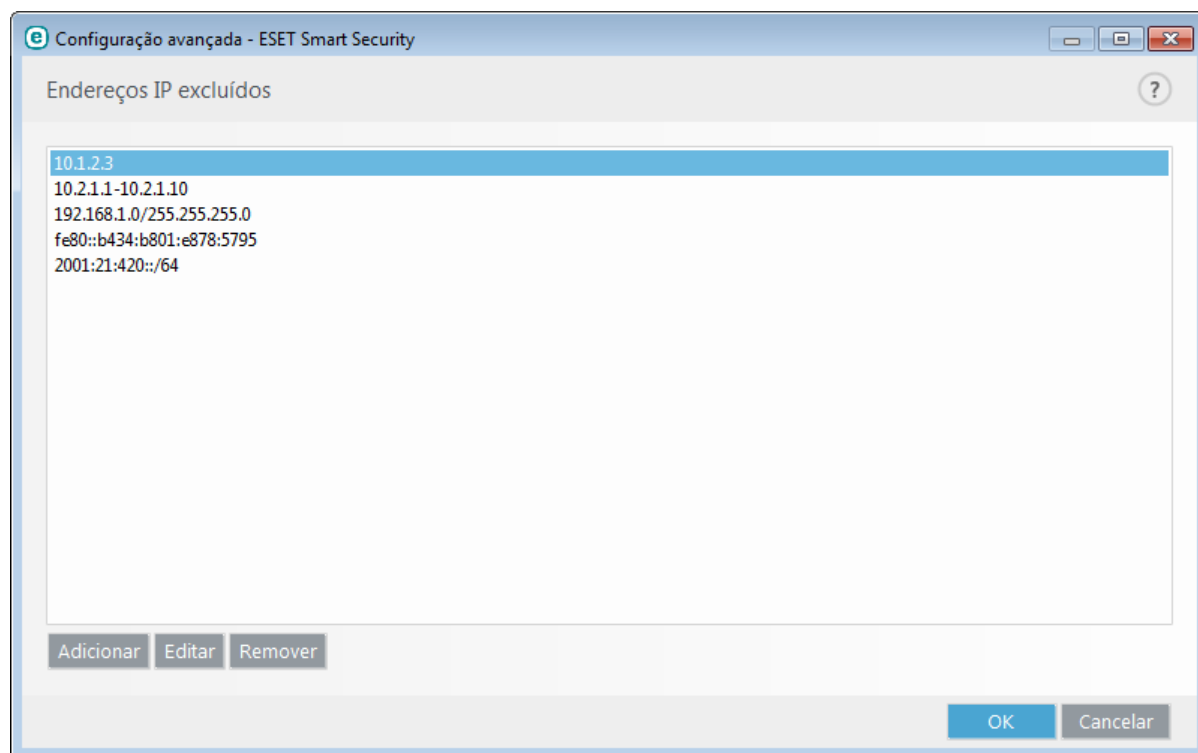
4.2.3.2 Aplicativos excluídos

Para excluir da filtragem de conteúdos a comunicação de aplicativos específicos que possuem direito de acesso à rede, selecione-os na lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos usar isto apenas para aplicativos que não funcionam corretamente se as suas comunicações estiverem sendo rastreadas.

A execução de aplicativos e serviços estará disponível automaticamente. Clique em **Adicionar** para adicionar um aplicativo manualmente se ele não for exibido na lista de filtragem de protocolo.

4.2.3.3 Endereços IP excluídos

As entradas na lista serão excluídas da filtragem de conteúdos do protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços conhecidos como sendo confiáveis.

Clique em **Adicionar** para excluir um endereço IP/intervalo de endereço/subrede de um ponto remoto para que não seja exibido na lista de filtragem de protocolo.

Clique em **Remover** para remover as entradas selecionadas da lista.

4.2.3.3.1 Adicionar endereço IPv4

Isso permite que você adicione um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra é aplicada. A versão 4 do IP (Internet Protocol) é a versão mais antiga, mas ainda é a mais amplamente utilizada.

Endereço único - Adiciona o endereço IP de um computador individual para o qual a regra será aplicada (por exemplo, *192.168.0.10*).

Intervalo de endereços - Digite o primeiro e último endereço IP para especificar o intervalo IP (de vários computadores) para o qual a regra será aplicada (por exemplo, *192.168.0.1* a *192.168.0.99*).

Sub-rede - Sub-rede (um grupo de computadores) definida por um endereço IP e máscara.

Por exemplo, *255.255.255.0* é a máscara de rede para o prefixo *192.168.1.0/24*, que significa o intervalo de endereços de *192.168.1.1* a *192.168.1.254*.

4.2.3.3.2 Adicionar endereço IPv6

Permite adicionar um endereço/sub-rede IPv6 de um ponto remoto para o qual a regra deve ser aplicada. É a versão mais recente do protocolo do IP (Internet Protocol) e substituirá a versão 4 mais antiga.

Endereço único - Adiciona o endereço IP de um computador individual para o qual a regra é aplicada (por exemplo *2001:718:1c01:16:214:22ff:fec9:ca5*).

Sub-rede - A sub-rede (um grupo de computadores) é definida por um endereço IP e máscara (por exemplo: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

O ESET Smart Security é capaz de verificar se há ameaças em comunicações que usam o protocolo SSL. É possível usar vários modos de rastreamento para examinar comunicações protegidas por SSL com certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Ativa filtragem de protocolo SSL/TLS - Se a filtragem de protocolo estiver desativada, o programa não rastreará as comunicações em SSL.

O **Modo de filtragem de protocolo SSL/TLS** está disponível nas seguintes opções:

> **Modo automático** - O modo automático vai rastrear apenas aplicativos adequados como navegadores da Web e clientes de email. É possível cancelar selecionando os aplicativos para os quais as comunicações serão rastreadas.
>
> **Modo interativo** - Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.
>
> **Modo de política** - Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado como confiável (ele está na lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

Lista de aplicativos SSL filtrados - Permite que você personalize o comportamento do ESET Smart Security para aplicativos específicos.

Lista de certificados conhecidos - Permite que você personalize o comportamento do ESET Smart Security para certificados SSL específicos.

Excluir comunicação protegida com Certificados de Validação Estendidos (EV) - Quando ativado, a comunicação com esse tipo de certificado SSL será excluída da verificação. Os Certificados SSL de Validação Estendida garantem que você está realmente vendo seu site, e não um site falso com a aparência exata do seu (típico para sites de roubo de identidade).

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2 - A comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

Certificado raiz

> **Adicionar o certificado raiz aos navegadores conhecidos** - Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). Quando ativado, o ESET Smart Security vai adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (por exemplo, no Internet Explorer).
>
> Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Validade do certificado

Caso o certificado não possa ser verificado usando o depósito de certificados TRCA - em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (TRCA). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria dos negócios de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Você pode selecionar **Bloquear a comunicação que utiliza o certificado** para sempre encerrar conexões criptografadas para sites com certificados não verificados.

Se o certificado não for válido ou estiver corrompido - Isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos que você deixe a opção **Bloquear a comunicação que utiliza o certificado** selecionada.

4.2.3.4.1 Certificados

Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). **Adicionar o certificado raiz aos navegadores conhecidos** deve estar ativado. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (ou seja, Internet Explorer). Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (por exemplo, VeriSign). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria dos negócios de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Uma caixa de diálogo de seleção de ação será exibida, na qual você decidirá marcar o certificado como confiável ou excluído. Se o certificado não estiver presente na lista TRCA, a janela estará vermelha. Se o certificado estiver na lista TRCA, a janela estará verde.

Você poderá selecionar **Bloquear a comunicação que utiliza o certificado** para terminar sempre uma conexão criptografada para o site que usa o certificado não verificado.

Se o certificado não for válido ou estiver corrompido, isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos o bloqueio da comunicação que usa o certificado.

4.2.3.4.2 Lista de certificados conhecidos

A **Lista de certificados conhecidos** pode ser usada para personalizar o comportamento do ESET Smart Security para certificados SSL específicos, bem como para lembrar ações escolhidas se o **Modo interativo** estiver selecionado no **Modo de filtragem de protocolo SSL/TLS**. A lista pode ser visualizada e editada em **Configuração avançada** (F5) > **Web e email** > **SSL/TLS** > **Lista de certificados conhecidos**.

A janela **Lista de certificados conhecidos** consiste em:

Colunas

Nome - Nome do certificado.

Emissor de certificado - Nome do autor do certificado.

Assunto do certificado - O campo de assunto identifica a entidade associada à chave pública armazenada no campo de chave pública do assunto.

Acesso - Selecione **Permitir** ou **Bloquear** como a **Ação de acesso** para permitir/bloquear a comunicação

protegida por este certificado, independentemente de sua confiabilidade. Selecione **Automático** para permitir certificados confiáveis e perguntar para não confiáveis. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Rastrear - Selecione **Rastrear** ou **Ignorar** como a **Ação de rastreamento** para rastrear ou ignorar a comunicação protegida por este certificado. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

Editar - Selecione o certificado que deseja configurar e clique em **Editar**.

Remover - Selecione o certificado que deseja excluir e clique em **Remover**.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** se quiser sair sem salvar.

4.2.3.4.3 Lista de aplicativos SSL filtrados

A **Lista de Lista de aplicativos SSL filtrados** pode ser usada para personalizar o comportamento do ESET Smart Security para aplicativos específicos, e para lembrar ações escolhidas se o **Modo interativo** estiver selecionado no **Modo de filtragem de protocolo de SSL**. A lista pode ser visualizada e editada em **Configuração avançada** (F5) > **Web e email** > **SSL/TLS** > **Lista de aplicativos SSL filtrados**.

A janela **Lista de aplicativos SSL filtrados** é composta por:

Colunas

Aplicativo - Nome do aplicativo.

Ação de rastreamento - Selecione **Rastrear** ou **Ignorar** para rastrear ou ignorar a comunicação. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

Adicionar - Adicionar aplicativo filtrado.

Editar - Selecione o certificado que deseja configurar e clique em **Editar**.

Remover - Selecione o certificado que deseja excluir e clique em **Remover**.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clique em **Cancelar** se quiser sair sem salvar.

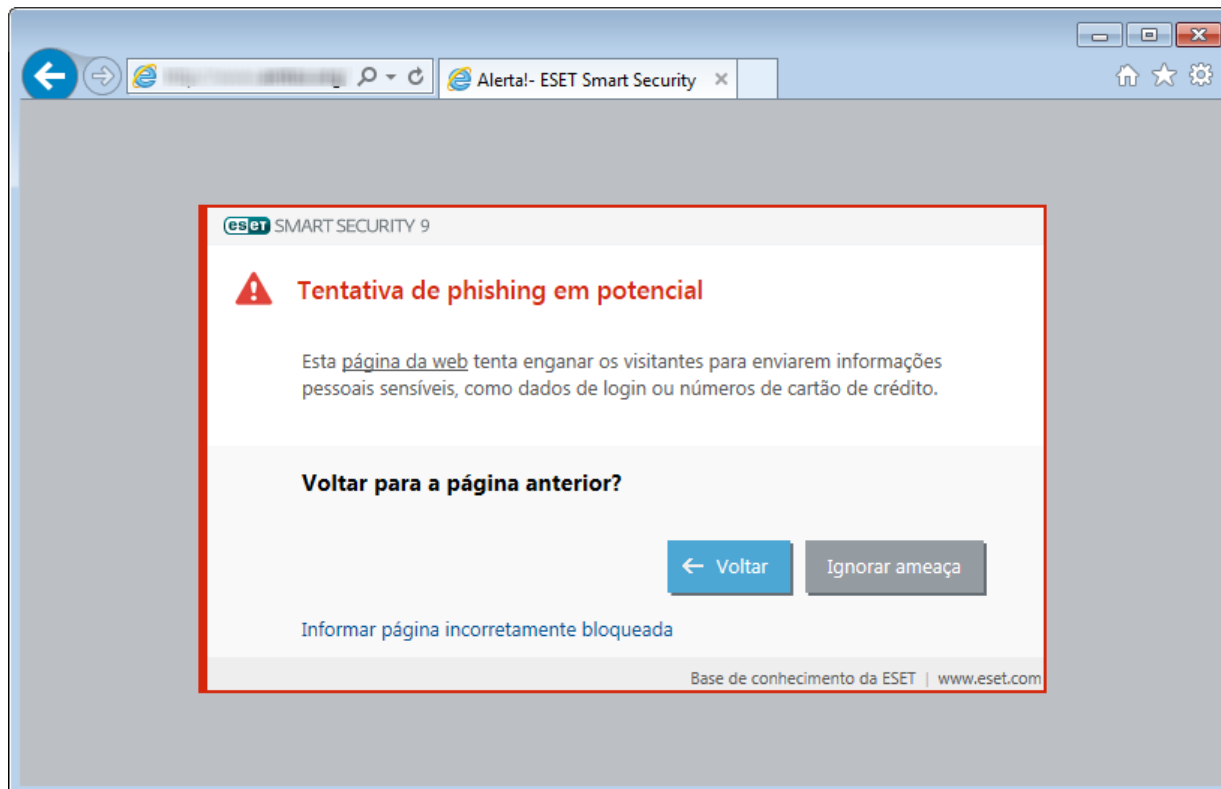
4.2.4 Proteção antiphishing

O termo roubo de identidade define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre essa atividade no glossário. O ESET Smart Security oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

Recomendamos que você ative a proteção antiphishing no ESET Smart Security. Para isso, abra a **Configuração avançada** (F5) e vá para **Web e email** > **Proteção antiphishing**.

Visite nosso artigo da Base de conhecimento para mais informações sobre a Proteção antiphishing no ESET Smart Security.

Acessando um site de roubo de identidade

Ao acessar um site de roubo de identidade reconhecido, você verá a caixa de diálogo a seguir no seu navegador da web. Se ainda quiser ter acesso ao site, clique em **Ignorar ameaça** (não recomendável).

OBSERVAÇÃO: por padrão, sites de roubo de identidade em potencial que tiverem sido permitidos expirarão horas depois. Para permitir um site permanentemente, use a ferramenta de gerenciamento de endereços de URL. A partir de **Configuração avançada** (F5) abra **Web e email** > **Proteção do acesso à Web** > **Gerenciamento de endereços URL** > **Lista de endereços**, clique em **Editar** e adicione o site que deseja editar na lista.

Denúncia de site de roubo de identidade

O link Denunciar permite que você denuncie um site de phishing/malicioso para análise da ESET.

OBSERVAÇÃO: antes de enviar um site para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o site não foi detectado,
- o site foi detectado incorretamente como uma ameaça. Nesse caso, você pode Informar página incorretamente bloqueada.

Como alternativa, você pode enviar o site por email. Envie seu email para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o site (por exemplo, o site do qual você foi enviado, como ouviu falar sobre ele, etc.).

4.3 Proteção de rede

O firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços. Ele também fornece proteção antivírus para protocolos HTTP, POP3 e IMAP. Esta funcionalidade representa um elemento muito importante na segurança do computador.

A configuração do firewall pessoal pode ser encontrada no painel **Configurar** em **Proteção de rede**. Aqui, é possível ajustar o modo de filtragem, regras e configurações detalhadas. Você também pode acessar mais configurações detalhadas clicando na roda de engrenagem ⚙ > **Configurar** ao lado de **Firewall pessoal** ou pressionando **F5** para acessar Configuração avançada.

Clique na roda de engrenagem ⚙ ao lado do **Firewall pessoal** para acessar as seguintes configurações:

Configurar... - Abre a janela Firewall pessoal na Configuração avançada, que permite definir como o firewall tratará a comunicação de rede.

Pausar firewall (permitir todo o tráfego) - O contrário do bloqueio de todo o tráfego de rede. Se ela for selecionada, todas as opções de filtragem do firewall pessoal serão desativadas, e todas as conexões de entrada e de saída serão permitidas. Clique em **Ativar firewall** para reativar o firewall enquanto a filtragem de tráfego de rede está neste modo.

Bloquear todo o tráfego - Todas as comunicação de entrada e saída serão bloqueadas pelo firewall pessoal. Utilize essa opção somente se suspeitar de riscos de segurança críticos que requeiram a desconexão do sistema da rede. Embora a filtragem de tráfego de rede esteja no modo **Bloquear todo o tráfego**, clique em **Parar de bloquear todo o tráfego** para restaurar a operação normal do firewall.

Modo automático - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem automático (com regras definidas pelo usuário).

Modo interativo - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem interativo.

Proteção contra ataque de rede (IDS) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Tráfego que seja considerado perigoso será bloqueado.

Proteção contra botnet - identifica malware de forma rápida e precisa no seu sistema.

Redes conectadas - Mostra as redes às quais os adaptadores de rede estão conectados. Depois de clicar no link abaixo do nome da rede, você será solicitado a selecionar um tipo de proteção (estrito ou permitido) para a rede à qual você está conectado via seu adaptador de rede. Essa configuração define o quanto seu computador é acessível para outros computadores na rede.

Lista de proibições temporária de endereços de IP - Veja uma lista de endereços de IP que foram detectados como a fonte de ataques e adicionados à lista de proibições para bloquear a conexão por um período de tempo. Para mais informações, clique nessa opção e pressione F1.

Assistente de solução de problemas - Ajuda a resolver problemas de conectividade causados pelo Firewall pessoal da ESET. Para obter informações mais detalhadas, consulte Assistente de solução de problemas.

4.3.1 Firewall pessoal

O firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem especificadas. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços. Ele também fornece proteção antivírus para protocolos HTTP, POP3 e IMAP. Esta funcionalidade representa um elemento muito importante na segurança do computador.

Ativar o Firewall pessoal - Recomendamos deixar este recurso ativado para ter ainda mais proteção. Assim o tráfego de rede é rastreado em ambas as direções.

Ativar Proteção contra ataque de rede (IDS) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado.

Ativar proteção Botnet - Detecta e bloqueia comunicações associadas com comandos maliciosos e servidores de controle ao reconhecer padrões que indicam que um computador está infectado e um bot está tentando se comunicar.

Modo de filtragem - O comportamento do firewall é alterado com base no modo de filtragem. Os modos de filtragem também influenciam o nível de interação necessário do usuário. Os modos de filtragem a seguir estão disponíveis para o firewall pessoal do ESET Smart Security:

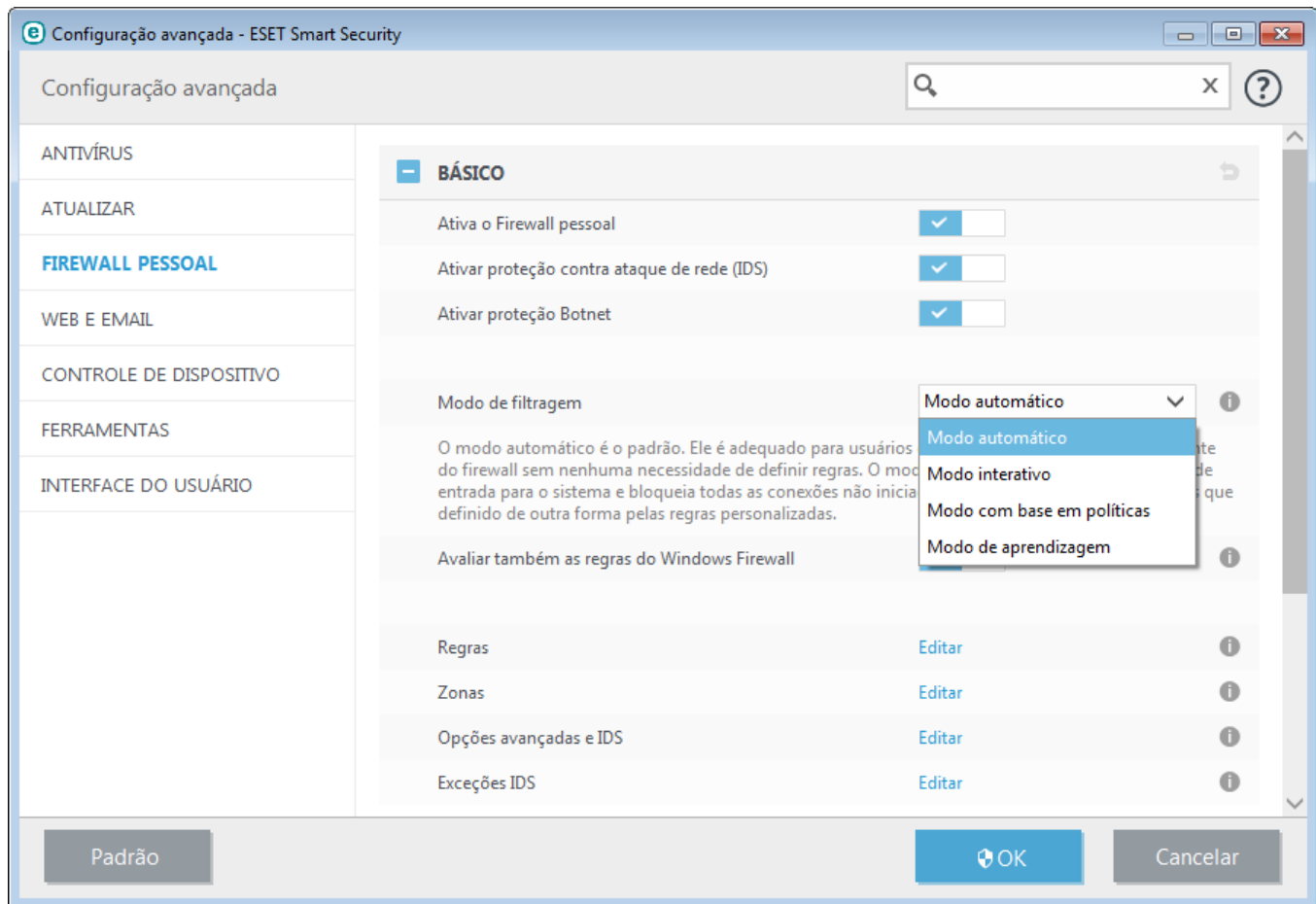
Modo automático - O modo padrão. Esse modo é adequado para usuários que preferem o uso fácil e conveniente do firewall sem necessidade de definir regras. Regras personalizadas e definidas pelo usuário podem ser criadas, mas não são exigidas no modo automático. O modo automático permite todo tráfego de saída para o sistema e bloqueia a maioria do tráfego de entrada (exceto algum tráfego da zona confiável, como especificado em IDS e opções avançadas/serviços permitidos e tráfego de entrada respondendo a comunicação de saída recente).

Modo interativo - Permite que você crie uma configuração personalizada para seu firewall pessoal. Quando uma comunicação para a qual não há regras aplicadas for detectada, será exibida uma janela de diálogo com a informação de uma conexão desconhecida. A janela de diálogo dá a opção de permitir ou negar a comunicação, e a decisão de permitir ou negar pode ser salva como uma nova regra para o firewall pessoal. Se o usuário escolher criar uma nova regra, todas as futuras conexões desse tipo serão permitidas ou bloqueadas de acordo com essa regra.

Modo com base em políticas - Bloqueia todas as conexões que não são definidas por uma regra específica que as permite. Esse modo permite que os usuários avançados definam as regras que permitem apenas as conexões desejadas e seguras. Todas as outras conexões não especificadas serão bloqueadas pelo firewall pessoal.

Modo de aprendizagem - Cria e salva automaticamente as regras e é adequado para a configuração inicial do firewall pessoal. Nenhuma interação com o usuário é exigida, porque o ESET Smart Security salva as regras de acordo com os parâmetros predefinidos. O modo de aprendizagem não deve ser apenas usado até que todas as regras para as comunicações exigidas tenham sido criadas para evitar riscos de segurança.

Perfis podem ser usados para personalizar o comportamento do firewall pessoal da ESET Smart Security ao especificar diferentes conjuntos de regras em diferentes situações.

Avaliar também regras de firewall do Windows - No modo automático, permite que o tráfego de entrada seja autorizado pelo Firewall do Windows a menos que tenha sido bloqueado pelas regras de firewall pessoal.

Regras - Aqui você pode adicionar regras e definir como o Firewall pessoal processará o tráfego de rede.

Zonas - Aqui você pode criar zonas que consistem em um ou vários endereços IP.

IDS e opções avançadas - Permite configurar opções avançadas de filtro e a funcionalidade IDS (usada para detectar vários tipos de ataques e vulnerabilidades).

Exceções IDS - Permite adicionar exceções IDS e personalizar reações a atividades maliciosas.

OBSERVAÇÃO:É possível criar uma exceção IDS quando o Botnet atacar seu computador. Uma exceção pode ser modificada em **Configuração avançada** (F5) > **Firewall pessoal** > **Exceções IDS**.

4.3.1.1 Configurações do modo de aprendizagem

O modo de aprendizagem cria e salva automaticamente uma regra para cada comunicação que foi estabelecida no sistema. Nenhuma interação com o usuário é exigida, porque o ESET Smart Security salva as regras de acordo com os parâmetros predefinidos.

Esse modo pode expor seu sistema a risco e é recomendado somente para configuração inicial do firewall pessoal.

Ative o Modo de aprendizagem em **Configuração avançada** (F5) > **Firewall pessoal** > **Configurações do modo de aprendizagem** para exibir as opções do Modo de aprendizagem. Essa seção inclui os seguintes itens:

Aviso: Enquanto está no Modo de aprendizagem, o firewall pessoal não filtra a comunicação. Todas as comunicações de saída e de entrada são permitidas. Nesse modo, o seu computador não está totalmente protegido pelo firewall pessoal.

Tipo de comunicação - Selecione os parâmetros específicos de criação de regras para cada tipo de comunicação. Há quatro tipos de comunicação:

Tráfego de entrada da zona Confiável - Um exemplo de uma conexão de entrada na zona confiável seria um computador remoto a partir do qual a zona confiável está tentando estabelecer comunicação com um aplicativo local em execução no seu computador.

Tráfego de saída para zona Confiável - Um aplicativo local está tentando estabelecer uma conexão com outro computador na rede local ou em uma rede na zona confiável.

Tráfego de entrada da Internet - Um computador remoto tentando se comunicar com um aplicativo em execução no computador.

Tráfego de saída da Internet - Um aplicativo local está tentando estabelecer uma conexão com outro computador.

Cada seção permite que você defina parâmetros a serem adicionados às regras recém-criadas:

Adicionar porta local - Inclui o número da porta local da comunicação de rede. Para as comunicações de saída, números aleatórios são frequentemente gerados. Por essa razão, recomendamos a ativação dessa opção apenas para as comunicações de entrada.

Adicionar aplicativo - Inclui o nome do aplicativo local. Essa opção é adequada para regras de nível de aplicativo (regras que definem a comunicação para um aplicativo inteiro). Por exemplo, é possível ativar a comunicação apenas para um navegador da Web ou cliente de email.

Adicionar porta remota - Inclui o número da porta remota da comunicação de rede. Por exemplo, você pode permitir ou negar um serviço específico associado a um número de porta padrão (HTTP - 80, POP3 - 110, etc.).

Adicionar endereço IP remoto/Zona confiável - Um endereço IP ou uma zona remoto(a) pode ser utilizado(a) como um parâmetro para novas regras que definem todas as conexões de rede entre o sistema local e esse endereço/ zona remoto(a). Essa opção é adequada se você desejar definir ações para determinado computador ou grupo de computadores conectados em rede.

Número máximo de regras diferentes para um aplicativo - Se um aplicativo comunicar por meio de diferentes portas para vários endereços IP etc., o firewall no modo de aprendizagem criará uma contagem apropriada de regras para esse aplicativo. Essa opção permite limitar o número de regras que podem ser criadas para um aplicativo.

4.3.2 Perfis do firewall

Os perfis podem ser usados para controlar o comportamento do firewall pessoal do ESET Smart Security. Ao criar ou editar uma regra de firewall pessoal, você pode atribuí-la a um perfil específico ou aplicá-la a cada perfil. Quando um perfil está ativo em uma interface de rede, apenas as regras globais (regras sem nenhum perfil especificado) e as regras que foram atribuídas a esse perfil são aplicadas a ele. Você pode criar vários perfis com regras diferentes atribuídas a adaptadores de rede ou atribuídas a redes para alterar com facilidade o comportamento do firewall pessoal.

Clique em **Editar** ao lado de **Lista de perfis** para abrir a janela **Perfis do firewall**, onde é possível editar perfis.

Um adaptador de rede pode ser configurado para usar um perfil configurado para uma rede específica quando estiver conectado a essa rede. Você também pode atribuir um perfil específico para uso quando em uma determinada rede em **Configuração avançada** (F5) > **Firewall pessoal** > **Redes conhecidas**. Selecione uma rede da lista de **Redes conhecidas** e clique em **Editar** para atribuir um perfil de firewall para a rede específica no menu suspenso **Perfil de firewall**. Se essa rede não tiver um perfil atribuído, então o perfil padrão do adaptador será usado. Se o adaptador for configurado para usar o perfil da rede, seu perfil padrão será usado, independentemente de à qual rede estiver conectado. Se não houver perfil da rede nem da configuração do adaptador, o perfil global padrão é usado. Para atribuir um perfil a um adaptador de rede, selecione o adaptador de rede, clique em **Editar** ao lado de**Perfis atribuídos a adaptadores de rede**, selecione o perfil do menu suspenso **Perfil de firewall padrão** e clique em **Salvar**.

Quando o firewall pessoal alternar para outro perfil, uma notificação será exibida no canto inferior direito próximo ao relógio do sistema.

4.3.2.1 Perfis atribuídos a adaptadores de rede

Ao alternar perfis, você pode fazer rapidamente várias mudanças no comportamento do firewall. Regras personalizadas podem ser definidas e aplicadas para perfis específicos. Entradas do adaptador de rede para todos os adaptadores presentes na máquina são adicionadas automaticamente à lista de **Adaptadores de rede**.

Colunas

Nome - Nome do adaptador de rede.

Perfil de firewall padrão - O perfil padrão é usado quando a rede à qual você está conectado não tem um perfil configurado ou se o adaptador de rede estiver configurado para não usar o perfil de rede.

Perfil de rede preferido - Quando a opção **Dar preferência ao perfil de firewall da rede conectada** for ativada, o adaptador de rede usará o perfil de firewall atribuído a uma rede conectada sempre que possível.

Elementos de controle

Adicionar - Adiciona um novo adaptador de rede.

Editar - Permite editar um adaptador de rede existente.

Remover - Selecione um adaptador de rede e clique em **Remover** se quiser remover um adaptador de rede da lista.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clicar em **Cancelar** para sair sem fazer alterações.

4.3.3 Configuração e uso de regras

As regras representam um conjunto de condições utilizadas para testar significativamente todas as conexões de rede e todas as ações atribuídas a essas condições. Usando regras de firewall pessoal é possível definir a ação a ser feita quando diferentes tipos de conexões de rede são estabelecidos. Para acessar a configuração de filtragem de regras, navegue até **Configuração avançada** (F5) > **Firewall pessoal** > **Básico**. Algumas das regras predefinidas são vinculadas às caixas de seleção de **serviços permitidos** (Opções avançadas e IDS) e elas não podem ser desativadas diretamente; em vez disso, você pode usar essas caixas de seleção relacionadas para fazer isso.

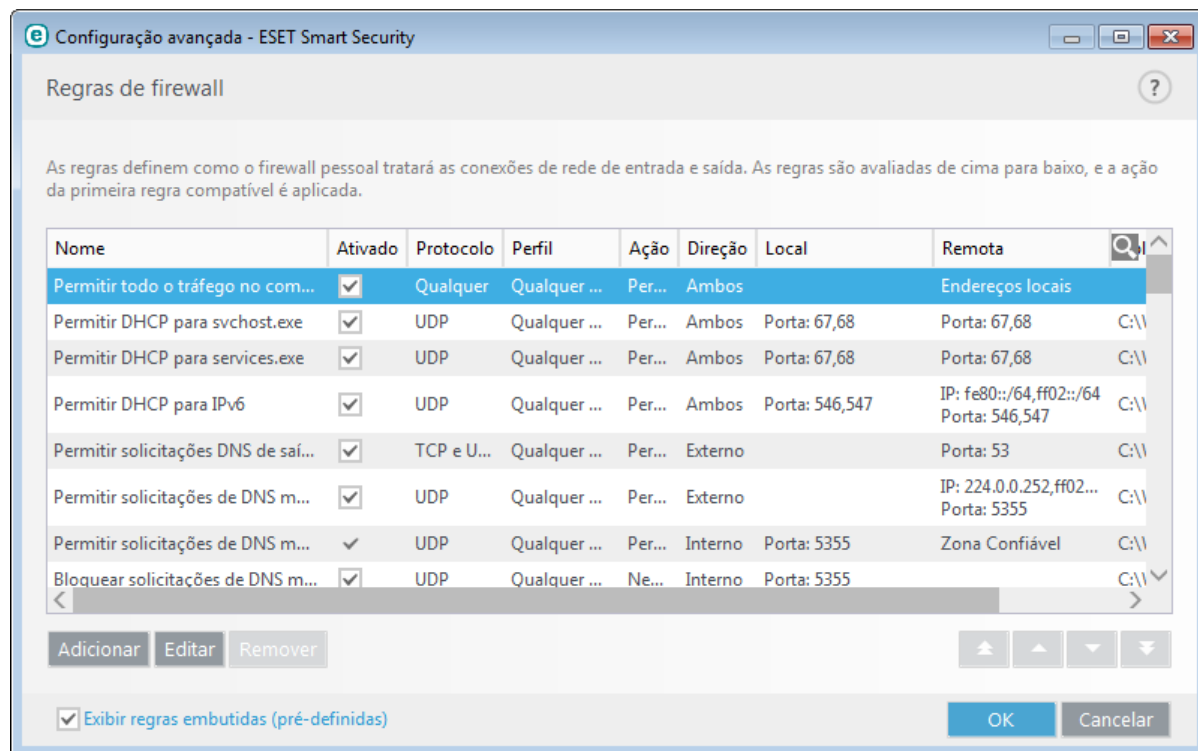
Ao contrário da versão anterior do ESET Smart Security, regras são avaliadas do início para o fim. A ação da primeira regra correspondente é usada para cada conexão de rede sendo avaliada. Essa é uma alteração comportamental importante da versão anterior na qual a prioridade de regras era automática e regras mais específicas tinham prioridade superior do que as mais gerais.

As conexões podem ser divididas em conexões de entrada e de saída. As conexões de entrada são iniciadas por um computador remoto que tenta estabelecer uma conexão com o sistema local. As conexões de saída funcionam de maneira oposta - o sistema local contata um computador remoto.

Se uma nova comunicação desconhecida for detectada, é preciso considerar cuidadosamente se vai permiti-la ou negá-la. As conexões não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se tal conexão for estabelecida, recomenda-se que seja dada atenção especial ao computador remoto e ao aplicativo tentando conectar-se ao computador. Muitas ameaças tentam obter e enviar dados particulares ou fazem download de outros aplicativos maliciosos para o computador/sistema local. O firewall pessoal permite que o usuário detecte e finalize tais conexões.

4.3.3.1 Regras de firewall

Clique em **Editar** ao lado de **Regras** na seção da guia **Básico** para exibir a janela **Regras de firewall**, onde a lista de todas as regras é exibida. **Adicionar**, **Editar** e **Remover** permite que você adicione, configure ou exclua regras. É possível ajustar o nível de prioridade de uma regra selecionando a regra e clicando em **Início/Para cima/Final/Para baixo**.

DICA: Você pode usar o campo **Pesquisar** para encontrar uma regra por nome, protocolo ou porta.

Colunas

Nome - Nome da regra.

Ativado - Mostra se regras estão ativadas ou desativadas, a caixa de seleção correspondente deve ser selecionada para ativar uma regra.

Protocolo - O protocolo para o qual esta regra é válida.

Perfil - Mostra o perfil de firewall para o qual esta regra é válida.

Ação - Mostra o status da comunicação (bloquear/permitir/perguntar).

Direção - Direção da comunicação (entrada/saída/ambas).

Local - Endereço IP e porta do computador local.

Remoto - Endereço IP e porta do computador remoto.

Aplicativos -O aplicativo ao qual a regra se aplica.

Elementos de controle

Adicionar -Cria uma nova regra.

Editar - Permite editar as regras existentes.

Remover - Remove as regras existentes.

Exibir regras embutidas (predefinidas) - Regras predefinidas por ESET Smart Security que permitem ou negam comunicações específicas. Você pode desativar essas regras, mas você não pode excluir uma regra predefinida.

Início/Para cima/Final/Para baixo- Permite que você ajuste o nível de prioridade de regras (regras são executadas

do início para o fim).

4.3.3.2 Trabalhando com regras

A modificação é necessária toda vez que os parâmetros monitorados são alterados. Se forem feitas alterações de forma que uma regra não preenche completamente as condições e a ação especificada não pode ser aplicada, a conexão determinada pode ser negada. Isso pode resultar em problemas com o funcionamento do aplicativo afetado por uma regra. Um exemplo é uma alteração do endereço de rede ou do número de porta para o local/ endereço remoto.

A parte superior da janela contém três guias:

- **Geral** - Especifica um nome de regra, a direção da conexão, a ação (**Permitir**, **Negar**, **Perguntar**), o protocolo e o perfil ao qual a regra se aplicará.
- **Local** - Exibe informações sobre o lado local da conexão, incluindo o número da porta local ou o intervalo de portas e o nome do aplicativo de comunicação. Também permite que você adicione uma zona pré-definida ou criada com um intervalo de endereços IP aqui, ao clicar em **Adicionar**.
- **Remoto** - Esta guia contém informações sobre a porta remota (intervalo de portas). Permite que você defina uma lista de endereços IP remotos ou zonas para uma determinada regra. Você também pode adicionar uma zona pré-definida ou criada com um intervalo de endereços IP aqui, ao clicar em **Adicionar**.

Ao criar uma nova regra, é preciso digitar o nome da regra no campo **Nome**. Selecione a direção para a qual a regra se aplica no menu suspenso **Direção** e a ação a ser executada quando um canal de comunicação encontra a regra no menu suspenso **Ação**.

Protocolo representa o protocolo de transferência usado para a regra. Selecione qual protocolo usar para determinada regra do menu suspenso.

Código/tipo ICMP representa uma mensagem ICMP identificada por um número (por exemplo, 0 representa "resposta Echo").

Por padrão, todas as regras estão ativadas para **Qualquer perfil**. Alternativamente, selecione um perfil de firewall personalizado usando o menu suspenso **Perfil**.

Se ativar o **Reportar**, a atividade conectada com a regra será registrada em um relatório. **Notificar usuário** exibe uma notificação quando a regra é aplicada.

DICA: A seguir é apresentado um exemplo no qual criamos uma nova regra para permitir que o aplicativo do navegador da Web acesse a rede. O seguinte deve ser configurado:

- Na guia **Geral**, ative a comunicação de saída por meio dos protocolos TCP e DP.
- Adicione o aplicativo do seu navegador (para o Internet Explorer, é iexplore.exe) na guia **Local**.
- Na guia **Remoto**, ative a porta número 80 se você deseja permitir navegação padrão na Internet.

OBSERVAÇÃO: Esteja ciente de que regras pré-definidas podem ser modificadas de forma limitada.

4.3.4 Configuração de zonas

Uma zonas representa uma coleção de endereços de rede que criam um grupo lógico de endereços IP, úteis quando você precisa reutilizar o mesmo conjunto de endereços em várias regras. A cada endereço no grupo são atribuídas regras semelhantes definidas centralmente para todo o grupo. Um exemplo de tal grupo é a **Zona confiável**. Uma Zona confiável representa um grupo de endereços de rede que não são bloqueados pelo firewall pessoal de maneira alguma. Essas zonas podem ser configuradas em **Configuração avançada** > **Firewall pessoal** > **Básico**, clicando em **Editar** ao lado de **Zonas**. Para adicionar uma nova zona, clique em **Adicionar**, insira um **Nome** para a zona, uma **Descrição** e adicione um endereço IP remoto no campo **Endereço do computador remoto (IPv4/IPv6, intervalo, máscara)**.

Na janela de configuração **Zonas de firewall**, você pode especificar um nome de zona, descrição e lista de endereço de rede (consulte também Editor de redes conhecidas).

4.3.5 Redes conhecidas

Ao usar um computador que frequentemente se conecta a redes públicas ou redes fora de sua rede de trabalho normal, recomendamos que você verifique a credibilidade da rede de novas redes às quais está se conectando. Assim que as redes forem definidas, o ESET Smart Security poderá reconhecer redes confiáveis (Residencial/ comercial) usando vários parâmetros de rede configurados em **Identificação da rede**. Os computadores geralmente inserem redes com endereços IP semelhantes à rede confiável. Em tais casos, o ESET Smart Security pode considerar uma rede desconhecida como sendo confiável (Residencial/Comercial). Recomendamos que você use a **Autenticação de rede** para evitar esse tipo de situação.

Quando um adaptador de rede é conectado a uma rede ou suas configurações de rede são reconfiguradas, o ESET Smart Security pesquisará na lista de rede conhecida um registro que corresponda à nova rede. Se a **Identificação da rede** e a **Autenticação da rede** (opcional) corresponderem, a rede será marcada como conectada nesta interface. Quando nenhuma rede conhecida for encontrada, uma nova rede será criada na definição da configuração da identificação de rede para identificar a rede na próxima vez que você se conectar a ela. Por padrão, a nova conexão de rede usa o tipo de proteção **pública**. A janela do diálogo **Nova conexão de rede detectada** solicitará que você escolha entre o tipo de proteção **Pública** ou **Residencial/Comercial**. Se um adaptador de rede for conectado a uma rede conhecida e essa rede for marcada como **Residencial/Comercial**, sub-redes locais do adaptador serão adicionadas à Zona confiável.

OBSERVAÇÃO: Ao marcar "**Não perguntar o tipo de proteção das novas redes. Marcar automaticamente as novas redes como públicas**", a janela do diálogo **Nova conexão de rede detectada** não aparecerá e a rede à qual você está conectado será automaticamente marcada como pública. Isso fará com que determinados recursos (por exemplo, compartilhamento de arquivos e área de trabalho remota) fiquem inacessíveis de novas redes.

Redes conhecidas podem ser configuradas manualmente na janela Editor de redes conhecidas.

4.3.5.1 Editor de redes conhecidas

Redes conhecidas podem ser configuradas manualmente na janela **Configuração avançada** > **Firewall pessoal** > **Redes conhecidas** clicando em **Editar**.

Colunas

Nome - Nome da rede conhecida.

Tipo de proteção - Mostra se a rede está definida como **Doméstica/Trabalho** ou **Pública**.

Perfil do firewall - Selecione o perfil no menu suspenso **Exibir regras usadas no perfil** para exibir o filtro de regras de perfis.

Elementos de controle

Adicionar - Cria uma nova rede conhecida.

Editar - Clique para editar uma rede conhecida existente.

Remover - Selecione uma rede e clique em **Remover** para removê-la da lista de redes conhecidas.

Início/Para cima/Final/Para baixo - Permite que você ajuste o nível de prioridade de redes conhecidas (redes são avaliadas do início para o fim).

Definições de configuração de rede são divididas nas seguintes guias:

Rede

Aqui você pode definir o nome de rede e selecionar o tipo de proteção (**Pública** ou **Doméstica/Trabalho**) para a rede. Use o menu suspenso **Perfil de firewall** para selecionar o perfil para esta rede. Se a rede utilizar o tipo de proteção **Doméstica/Trabalho**, todas as sub-redes de rede conectadas diretamente serão consideradas confiáveis. Por exemplo, se um adaptador de rede for conectado a esse tipo de rede com o endereço IP 192.168.1.5 e a máscara de sub-rede 255.255.255.0, a sub-rede 192.168.1.0/24 será adicionada à zona confiável desse adaptador. Se o adaptador tiver mais endereços/sub-redes, todos eles serão confiáveis, independentemente da configuração **Identificação de rede** da rede conhecida.

Além disso, endereços adicionados em **Endereços adicionais confiáveis** serão sempre adicionados à zona confiável de adaptadores conectados a essa rede (independentemente do tipo de proteção da rede).

As seguintes condições devem ser atendidas para uma rede a ser marcada como conectada na lista de redes conectadas:

- Identificação de rede - Todos os parâmetros preenchidos devem corresponder aos parâmetros de conexão ativa.
- Autenticação de rede - se o servidor de autenticação for selecionado, a autenticação bem-sucedida com o servidor de autenticação ESET deverá ocorrer.
- Restrições de rede (somente Windows XP) - todas as restrições globais selecionadas deverão ser atendidas.

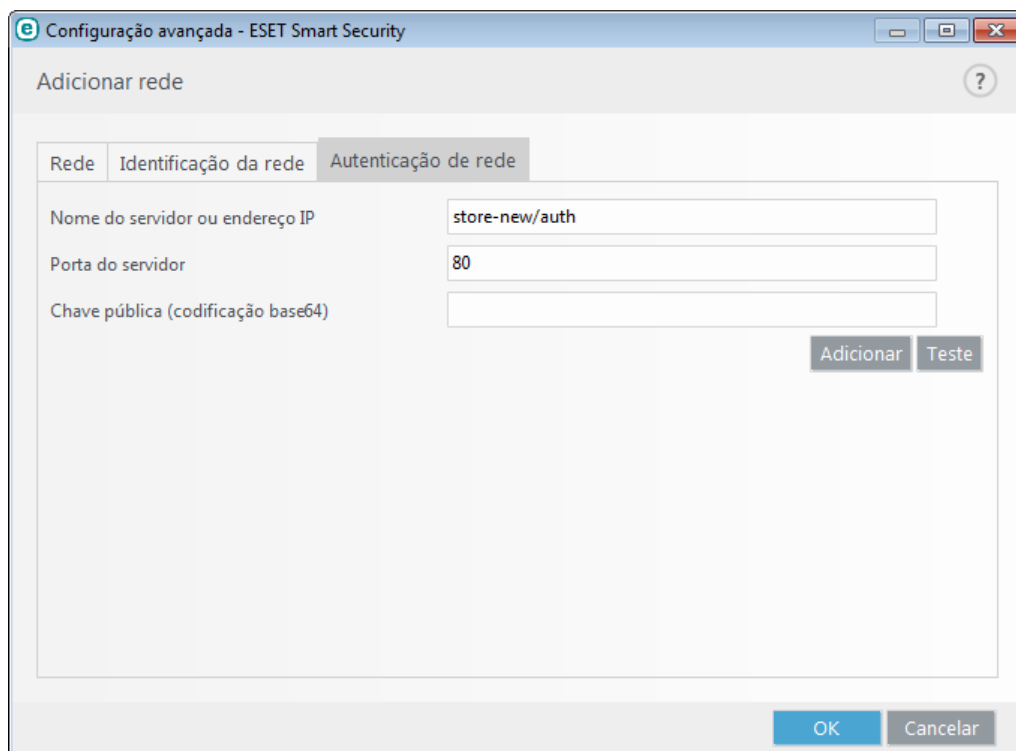
Identificação da rede

A identificação da rede é executada com base nos parâmetros do adaptador da rede local. Todos os parâmetros selecionados serão comparados em relação aos parâmetros reais de conexões de redes ativas. Endereços IPv4 e IPv6 serão permitidos.

Autenticação de rede

A autenticação de rede procura por um servidor específico na rede e usa uma criptografia assimétrica (RSA) para autenticar esse servidor. O nome da rede sendo autenticada deverá corresponder ao nome da zona definida em configurações do servidor de autenticação. O nome diferencia maiúsculas e minúsculas. Especifique um nome de servidor, uma porta de escuta do servidor e uma chave pública que corresponda à chave privada do servidor (consulte a seção Autenticação de rede - Configuração de servidor). O nome de servidor pode ser inserido na forma de um endereço IP, DNS ou nome NetBios e pode ser seguido por um caminho especificando o local da chave no servidor (por exemplo, server_name_/directory1/directory2/authentication). Você pode especificar servidores alternativos para uso acrescentando-os ao início do caminho, separados por ponto e vírgulas.

A chave pública pode ser importada usando qualquer um dos seguintes tipos de arquivos:

- Chave pública PEM codificada (.pem), essa chave pode ser gerada usando o servidor de autenticação ESET (consulte Autenticação de rede - Configuração de servidor).
- Chave pública codificada
- Certificado de chave pública (.crt)

Clique em **Testar** para testar suas configurações. Se a autenticação foi bem sucedida, *A autenticação do servidor foi bem sucedida* será exibido. Se a autenticação não estiver configurada corretamente, será exibida uma das seguintes mensagens de erro:

Falha na autenticação do servidor. Assinatura inválida ou sem correspondência.
A assinatura de servidor não corresponde à chave pública inserida.

Falha na autenticação do servidor. O nome da rede não corresponde.
O nome da rede configurada não corresponde ao nome da zona do servidor de autenticação. Verifique ambos os nomes e certifique-se de que sejam idênticos.

Falha na autenticação do servidor. Nenhuma resposta ou resposta inválida do servidor.
Uma resposta não será recebida se o servidor não estiver em execução ou não estiver acessível. Uma resposta inválida poderá ser recebida se outro servidor HTTP estiver em execução no endereço especificado.

Chave pública inválida inserida.
Verifique se o arquivo de chave pública inserido não está corrompido.

Restrições de rede (apenas para Windows XP)

Em sistemas operacionais modernos (Windows Vista e mais recentes), cada adaptador de rede tem sua própria zona confiável e perfil de firewall ativo. Infelizmente, no Windows XP, esse layout não é compatível; portanto, todos os adaptadores de rede sempre compartilham a mesma zona confiável e perfil de firewall ativo. Isso impõe um possível risco de segurança quando a máquina estiver conectada a várias redes simultaneamente. Nesses casos, o tráfego de uma rede não confiável pode ser avaliado usando a zona confiável e o perfil de firewall configurados para a outra rede conectada. Para minimizar qualquer risco de segurança, você pode usar as restrições a seguir para evitar aplicar globalmente uma configuração de rede enquanto outra rede (possivelmente não confiável) estiver conectada.

No Windows XP, configurações de rede conectadas (zona confiável e perfil de firewall) são aplicadas globalmente, exceto se pelo menos uma dessas restrições estiver ativada e não for atendida:

a. Apenas uma conexão ativa
b. Nenhuma conexão sem fio estabelecida
c. Nenhuma conexão insegura sem fio estabelecida

4.3.5.2 Autenticação de rede - Configuração de servidor

O processo de autenticação pode ser executado por qualquer computador/servidor conectado à rede que deva ser autenticado. O aplicativo Servidor de autenticação ESET precisa estar instalado em um computador/servidor que esteja sempre acessível para autenticação quando um cliente tentar se conectar à rede. O arquivo de instalação do aplicativo Servidor de autenticação ESET está disponível para download no site da ESET.

Depois de instalar o aplicativo Servidor de autenticação ESET, uma janela de diálogo será exibida (você pode acessar o aplicativo clicando em **Iniciar** > **Programas** > **ESET** > **Servidor de autenticação ESET**).

Para configurar o servidor de autenticação, insira o nome da zona de autenticação, a porta de escuta do servidor (o padrão é 80), bem como o local para armazenar o par de chaves pública e privada. Em seguida, gere as chaves pública e privada que serão utilizadas no processo de autenticação. A chave privada permanecerá no servidor, enquanto a chave pública precisará ser importada no lado do cliente na seção de autenticação da zona, ao definir uma zona na configuração do firewall.

Para informações mais detalhadas, leia o seguinte artigo na Base de conhecimento ESET.

4.3.6 Registro em log

O firewall pessoal do ESET Smart Security salva eventos importantes em um arquivo de log, que pode ser exibido diretamente no menu principal do programa. Clique em **Ferramentas** > **Mais ferramentas** > **Relatórios** e selecione **Firewall pessoal** no menu suspenso **Relatório**.

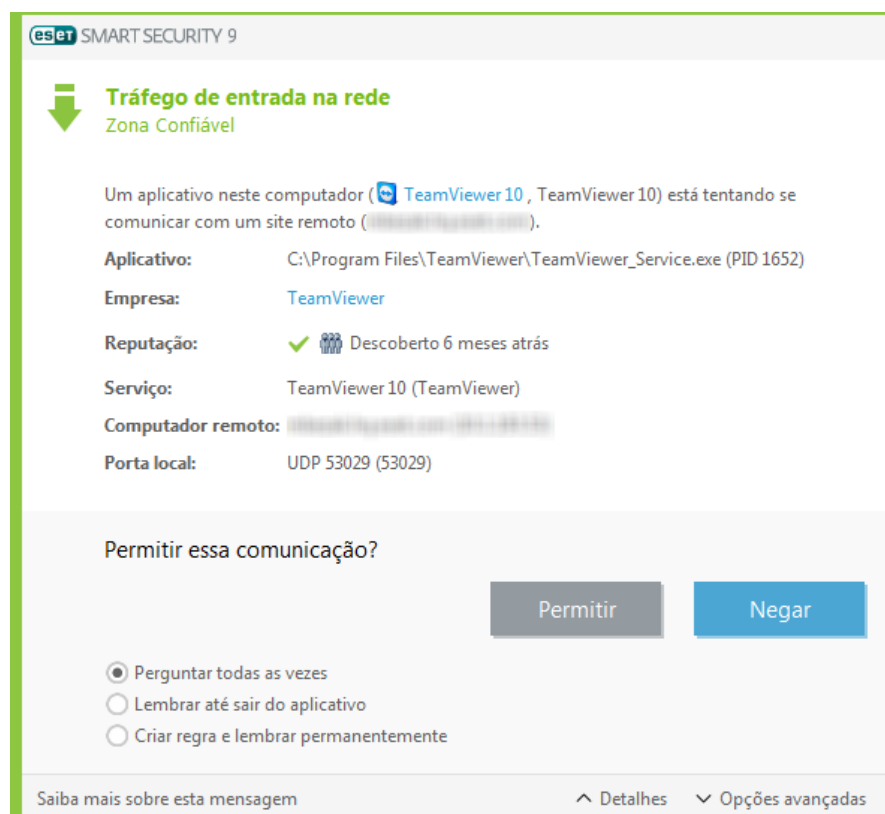
Os arquivos de log podem ser usados para detectar erros e revelar intrusos dentro do sistema. Os logs da firewall pessoal da ESET contêm os seguintes dados:

- Data e hora do evento
- Nome do evento
- Origem
- Endereço da rede de destino
- Protocolo de comunicação de rede
- Regra aplicada, ou nome do worm, se identificado
- Aplicativo envolvido
- Usuário

Uma análise completa desses dados pode ajudar a detectar tentativas de se comprometer a segurança do sistema. Muitos outros fatores indicam riscos de segurança potenciais e permitem que você reduza seus impactos: conexões frequentes de locais desconhecidos, diversas tentativas para estabelecer conexões, aplicativos desconhecidos comunicando-se ou números de portas incomuns sendo utilizados.

4.3.7 Estabelecimento de uma conexão - detecção

O firewall pessoal detecta cada conexão de rede recém-criada. O modo de firewall ativo determina quais ações serão executadas para a nova regra. Se o **Modo automático** ou o **Modo com base em políticas** estiver ativado, o firewall pessoal executará ações predefinidas sem nenhuma interação com o usuário.

O modo interativo exibe uma janela de informações que reporta a detecção de uma nova conexão de rede, suplementada com informações detalhadas sobre a conexão. O usuário pode escolher permitir a conexão ou recusá-la (bloqueio). Se houver necessidade de permitir várias vezes a mesma conexão na janela de diálogo, recomendamos que você crie uma nova regra para a conexão. Para isso, selecione **Criar regra e lembrar permanentemente**e salve a ação como uma nova regra para o firewall pessoal. Se o firewall reconhecer a mesma conexão no futuro, ele aplicará a regra existente sem solicitar a interação do usuário.

Tenha cuidado ao criar novas regras e permita apenas as conexões que você sabe que são seguras. Se todas as conexões forem permitidas, então o firewall pessoal falhará em realizar seu propósito. Estes são os parâmetros importantes para as conexões:

- **Lado remoto** - Somente permita conexões para endereços confiáveis e conhecidos.
- **Aplicativo local** - Não é aconselhável permitir conexões para aplicativos e processos desconhecidos.
- **Número da porta** - Em circunstâncias normais, a comunicação em portas comuns (como, por exemplo, o tráfego da web - porta 80) deve ser permitida.

Para se proliferar, as ameaças de computador usam frequentemente a Internet e conexões ocultas para ajudar a infectar sistemas remotos. Se as regras forem configuradas corretamente, um firewall pessoal se tornará uma ferramenta útil para a proteção contra diversos ataques de códigos maliciosos.

4.3.8 Resolvendo problemas com o firewall pessoal da ESET

Se você estiver tendo problemas de conectividade com o ESET Smart Security instalado, há várias formas de saber se o Firewall pessoal da ESET está causando o problema. Além disso, o Firewall pessoal da ESET pode ajudar você a criar novas regras ou exceções para resolver problemas de conectividade.

Consulte os seguintes tópicos para obter ajuda com a solução de problemas com o firewall pessoal da ESET:

- Assistente para solução de problemas
- Registrando e criando regras ou exceções de relatório
- Criando exceções de notificações do firewall
- Registro em relatório PCAP avançado
- Resolvendo problemas com a filtragem de protocolo

4.3.8.1 Assistente para solução de problemas

O assistente de solução de problemas monitora em segundo plano todas as conexões bloqueadas. Ele o orienta no processo de solução de problemas para corrigir problemas de firewall com dispositivos ou aplicativos específicos. Depois disso, ele sugere um novo conjunto de regras a serem aplicadas caso você as aprove. O **Assistente de solução de problemas** pode ser acessado no menu principal em **Configuração** > **Proteção de rede**.

4.3.8.2 Registrando e criando regras ou exceções de relatório

Por padrão, o Firewall pessoal da ESET não registra todas as conexões bloqueadas. Se você quiser ver o que foi bloqueado pelo Firewall pessoal, ative o registro em relatório na seção **Configuração avançada** em **Ferramentas** > **Diagnóstico** > **Ativar registro em relatório avançado de firewall pessoal**. Se você vir algo no relatório que não queira que o firewall pessoal bloqueie, poderá criar uma regra ou exceção de IDS para isso clicando com o botão direito do mouse nesse item e selecionando **Não bloquear eventos similares no futuro**. Observe que o relatório de todas as conexões bloqueadas pode conter milhares de itens e pode dificultar a localização de uma conexão específica nesse relatório. Você pode desativar o registro em relatório depois de resolver o problema.

Para obter mais informações sobre o relatório, consulte Relatórios.

OBSERVAÇÃO: Use o registro em relatório para ver o pedido no qual o Firewall pessoal bloqueou conexões específicas. Além disso, criar regras a partir do relatório permite que você crie regras que façam exatamente o que você deseja.

4.3.8.2.1 Criar regra de relatório

A nova versão do ESET Smart Security permite que você crie uma regra de relatório. No menu principal, clique em **Ferramentas** > **Mais ferramentas** > **Relatórios**. Escolha **Firewall pessoal** no menu suspenso, clique com o botão direito do mouse em sua entrada de relatório desejada e selecione **Não bloquear eventos similares no futuro** do menu de contexto. Uma janela de notificação exibirá sua nova regra.

Para permitir a criação de novas regras de relatório, o ESET Smart Security deve ser configurado com as seguintes configurações:

- define o detalhamento mínimo de registro em relatório como **Diagnóstico** em **Configuração avançada** (F5) > **Ferramentas** > **Relatórios**,
- ativar **Exibir notificações também para ataques sendo recebidos contra buracos de segurança** em **Configuração avançada** (F5) > **Firewall pessoal** > **IDS e opções avançadas** > **Detecção de intruso**.

4.3.8.3 Criando exceções de notificações do firewall pessoal

Quando o Firewall pessoal da ESET detectar atividade maliciosa na rede, uma janela de notificação descrevendo o evento será exibida. Esta notificação apresentará um link que permitirá que você saiba mais sobre o evento e configure uma exceção para ele caso queira.

OBSERVAÇÃO: se um dispositivo ou aplicativo em rede não implementar padrões de rede corretamente ele poderá acionar notificações de IDS do firewall repetidas. Você pode criar uma exceção diretamente da notificação para impedir que o Firewall pessoal da ESET detecte esse aplicativo ou dispositivo.

4.3.8.4 Registro em relatório PCAP avançado

Esse recurso tem como objetivo fornecer relatórios mais complexos para suporte ao cliente da ESET. Use esse recurso somente quando solicitado pelo suporte ao cliente da ESET, pois ele pode gerar um relatório enorme e deixar seu computador lento.

1. Vá para **Configuração avançada** > **Ferramentas** > **Diagnóstico** e ative **Ativar registro em relatório avançado de firewall pessoal**.
2. Tentativa de reproduzir o problema que você está tendo.
3. Desative o registro em relatório PCAP avançado.
4. O relatório PCAP pode ser encontrado no mesmo diretório no qual despejos de memória de diagnóstico são gerados:

- Microsoft Windows Vista ou mais recente

  C:\ProgramData\ESET\ESET Smart Security\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

4.3.8.5 Resolvendo problemas com a filtragem de protocolo

Se você tiver problemas com seu navegador ou cliente de email, a primeira etapa é determinar se a filtragem de protocolo é responsável. Para fazer isso, tente desativar temporariamente a filtragem de protocolo na configuração avançada (lembre-se de ativá-la novamente depois de ter concluído; caso contrário, seu navegador e cliente de email ficarão desprotegidos). Se o problema desaparecer após desativá-la, há uma lista de problemas comuns e uma forma para resolvê-los:

Atualizar ou proteger problemas de comunicação

Se seu aplicativo avisar sobre a incapacidade de atualizar ou que um canal de comunicação não está seguro:

- Se você tiver filtragem de protocolo SSL ativada, tente desativá-la temporariamente. Se isso ajudar, você poderá continuar usando filtragem SSL e fazer o trabalho de atualização excluindo a comunicação problemática:
  Alterne o modo de filtragem de protocolo SSL para interativa. Execute a atualização novamente. Deve haver um diálogo informando você sobre tráfego de rede criptografado. Certifique-se de que o aplicativo corresponda ao que você está solucionando e o certificado pareça estar vindo do servidor do qual está atualizando. Em seguida, escolha lembrar a ação para esse certificado e clique em ignorar. Se não houver mais diálogos relevantes a serem exibidos, você poderá alternar o modo de filtragem de volta para automático e o problema deverá ser resolvido.
- Se o aplicativo em questão não for um navegador ou cliente de email, você poderá excluí-lo totalmente da filtragem de protocolo (fazer isso para o navegador ou cliente de email deixaria você exposto). Qualquer aplicativo que tenha tido sua comunicação filtrada anteriormente já deve estar na lista fornecida para você ao adicionar a exceção; portanto, fazer o acréscimo manualmente não deve ser necessário.

Problema ao acessar um dispositivo em sua rede

Se você não conseguir usar qualquer funcionalidade de um dispositivo em sua rede (isso poderia significar abrir uma página da Web de sua webcam ou reproduzir vídeo em um media player doméstico), tente adicionar os respectivos

IPv4 e IPv6 à lista de endereços excluídos.

Problemas com um site específico

Você pode excluir sites específicos de filtragem de protocolo usando o gerenciamento de endereços URL. Por exemplo, se você não conseguir acessar https://www.gmail.com/intl/en/mail/help/about.html, tente adicionar *gmail.com* à lista de endereços excluídos.

Erro "Alguns dos aplicativos capazes de importar o certificado raiz ainda estão em execução"

Quando você ativar a filtragem de protocolo SSL, o ESET Smart Security certifica-se de que aplicativos instalados confiem na forma como ele filtra protocolo SSL importando um certificado para a loja de certificados. Para alguns aplicativos, isso não é possível enquanto eles estiverem em execução. Isso inclui Firefox e Opera. Certifique-se de que nenhum deles esteja em execução (a melhor forma de fazer isso é abrir o Gerenciador de tarefas e certificar-se de que não haja firefox.exe ou opera.exe na guia Processos) e então tente novamente.

Erro sobre assinatura inválida ou emissor não confiável

Isso muito provavelmente significa que a importação descrita acima falhou. Primeiro, certifique-se de que nenhum dos aplicativos mencionados esteja em execução. Em seguida, desative a filtragem de protocolo SSL e a ative novamente. Isso executará novamente a importação.

4.4 Ferramentas de segurança

A configuração **Ferramentas de segurança** permite ajustar os módulos seguintes:

- Proteção de Atividade bancária e Pagamento
- Controle dos pais
- Antifurto

4.4.1 Controle dos pais

O módulo Controle dos pais permite configurar as definições do controle dos pais, fornecendo aos pais ferramentas automatizadas que ajudam a proteger as crianças e a definir restrições para dispositivos e serviços. O objetivo é impedir que as crianças e os jovens tenham acesso a páginas com conteúdos impróprios ou prejudiciais.

O Controle dos pais permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os pais podem proibir o acesso para mais de 40 categorias de site predefinidas e mais de 140 subcategorias.

Para ativar o Controle dos pais para uma conta de usuário específica, siga estas etapas:

1. Por padrão, o Controle dos pais está desabilitado no ESET Smart Security. Há dois métodos para ativar o Controle dos pais:
   - Clique em em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** na janela principal do programa e altere o estado do Controle dos pais para ativado.
   - Pressione F5 para acessar a árvore de **Configuração avançada**, vá para **Web e email** > **Controle dos pais** e em seguida selecione a opção ao lado de **Integrar ao sistema**.
2. Clique em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** na janela principal do programa. Mesmo que **Ativado** apareça ao lado de **Controle dos pais**, você deverá configurar o Controle dos pais para a conta desejada clicando em **Proteger esta conta**. Na janela de configuração da Conta, insira uma idade para determinar o nível de acesso e as páginas da web recomendadas para a faixa etária informada. O Controle dos pais agora será ativado para a conta de usuário especificada. Clique em **Conteúdo permitido e proibido...** em um nome de conta para personalizar categorias que você deseja permitir ou bloquear na guia Categorias. Para permitir ou bloquear páginas da web personalizadas que não correspondam a uma categoria, clique na guia Exceções.

Se clicar em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** na janela principal do produto do ESET Smart Security, você verá que a janela principal conta com:

Contas de usuário do Windows

Se você tiver criado uma função para uma conta existente, ela será exibida aqui. Clique no controle deslizante para que ele mostre uma marca de verificação verde ao lado do Controle dos pais da conta. Em uma conta ativa, clique em Conteúdo permitido e proibido... para ver a lista de categorias de páginas da web permitidas para essa conta, bem como páginas da web bloqueadas e permitidas.

Importante: Para criar uma nova conta (por exemplo, para uma criança), use as seguintes instruções passo a passo para o Windows 7 ou o Windows Vista:

1. Abra **Contas de usuário** clicando no botão **Iniciar** (localizado no lado esquerdo inferior de sua área de trabalho), clicando em **Painel de controle** e clicando em **Contas de usuário**.
2. Clique em **Gerenciar contas do usuário**. Se for solicitada uma confirmação ou senha do administrador, digite a senha ou forneça a confirmação.
3. Clique em **Criar nova conta**.
4. Digite o nome que quiser dar à conta de usuário, clique em um tipo de conta e clique em **Criar conta**.
5. Abra novamente o painel do controle dos pais clicando novamente na janela principal do programa do ESET Smart Security para **Configuração** > **Ferramentas de segurança** > **Controle dos pais**.

A parte inferior da janela contém

Adicionar uma exceção para um site... - O site específico pode ser permitido ou bloqueado de acordo com suas preferências para cada conta dos pais, separadamente.

Mostrar relatórios – Essa opção mostra um relatório detalhado da atividade de Controle dos pais (páginas bloqueadas, a conta, por que a página foi bloqueada, categoria, etc.). Também é possível filtrar esse relatório clicando em **Filtragem** de acordo com seus próprios critérios.

Controle dos pais

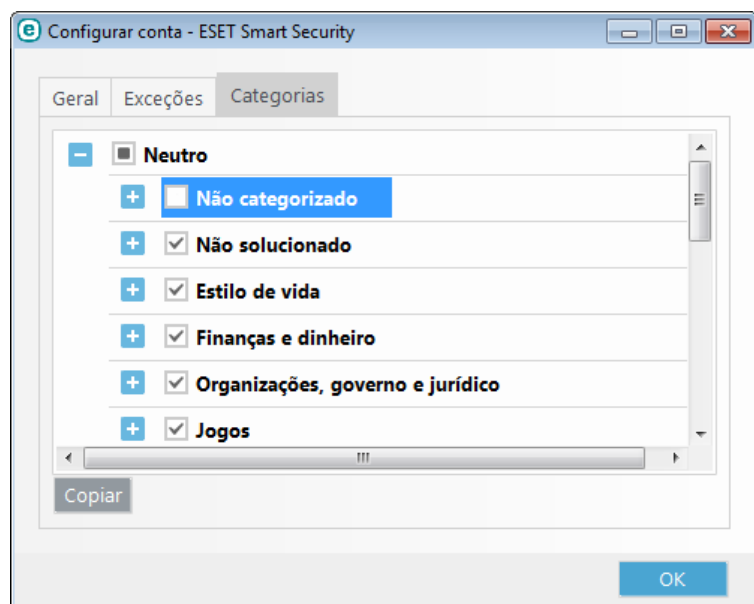
Depois de desativar o controle dos pais, uma janela **Desativar controle dos pais** vai aparecer. Aqui você pode definir o intervalo de tempo durante o qual a proteção estará desativada. A opção muda, então, para **Pausado** ou **Desativado permanentemente**.

É importante proteger as definições no ESET Smart Security com uma senha. Essa senha pode ser definida na seção Configuração de acesso. Se nenhuma senha for definida, o aviso a seguir será exibido - **Proteger o Controle dos pais com senha para impedir alterações não autorizadas**. As restrições definidas no Controle dos pais afetam apenas as contas de usuário padrão. Como um administrador pode substituir qualquer restrição, elas não terão nenhum efeito.

Por padrão, a comunicação HTTPS (SSL) não é filtrada. Portanto, o Controle dos pais não pode bloquear páginas da web que começam com *https://*. Para ativar este recurso, ative a configuração **Ativar filtragem de protocolo SSL/TLS** na árvore **Configuração avançada** em **Web e email** > **SSL/TLS**.

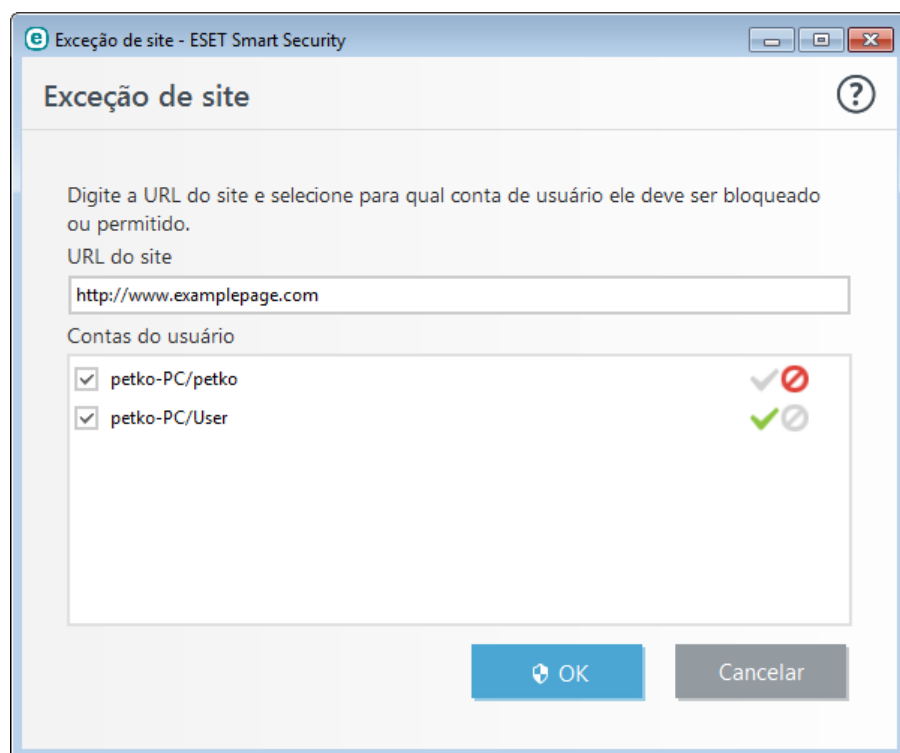
OBSERVAÇÃO: O controle dos pais requer que Filtragem de conteúdo do protocolo de aplicativo, Verificação de protocolo HTTP e Firewall pessoal estejam ativados para funcionar adequadamente. Por padrão, todas essas funcionalidades estão ativadas.

4.4.1.1 Categorias

Se a caixa de seleção ao lado de uma categoria estiver marcada, ela estará permitida. Desmarque a caixa de seleção próxima a uma categoria específica para bloqueá-la na conta selecionada.

Ao mover o mouse sobre uma categoria, será exibida uma lista de páginas da web que se enquadram nessa categoria. Aqui estão alguns exemplos de categorias (grupos) com os quais os usuários podem não estar familiarizados:

- **Diversos** - Geralmente, endereços IP privados (locais), como intranet, 127.0.0.0/8, 192.168.0.0/16, etc. Quando você recebe um código de erro 403 ou 404, o site também corresponderá a essa categoria.
- **Não solucionado** - Esta categoria inclui páginas da web não solucionadas devido a um erro ao se conectar ao mecanismo do banco de dados do Controle dos pais.
- **Não categorizado** - Páginas da web desconhecidas que ainda não estão no banco de dados.
- **Compartilhamento de arquivos** - Estas páginas da web contêm grandes quantidades de dados, como fotos, vídeos ou livros eletrônicos. Há um risco de que esses sites possam conter materiais potencialmente ofensivos ou de conteúdo adulto.

4.4.1.2 Exceções de site

Digite um URL no campo em branco na lista, selecione a caixa de seleção ao lado da conta de usuário, selecione ✔ ou ⊘ e clique em **Ok** para adicioná-lo à lista. Para excluir um endereço URL da lista, clique em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** > **Conteúdo permitido e proibido**. Na conta de usuário desejada, clique na guia **Exceção**, selecione a exceção e clique em **Remover**.

Na lista de endereço URL, os símbolos especiais * (asterisco) e ? (ponto de interrogação) não podem ser usados. Por exemplo, os endereços de página da Web com vários TLDs devem ser inseridos manualmente *(paginaexemplo.com*, *paginaexemplo.sk*, etc.). Quando você adiciona um domínio na lista, todo o conteúdo localizado neste domínio e em todos os subdomínios (por exemplo, *sub.paginaexemplo.com*) será bloqueado ou permitido de acordo com sua escolha de ação baseada na URL.

OBSERVAÇÃO: Bloquear ou permitir uma página da Web específica pode ser mais seguro do que bloquear ou permitir uma categoria de páginas da Web. Tenha cuidado ao alterar essas configurações e adicionar uma página da web ou categoria à lista.

4.5 Atualização do programa

Atualizar o ESET Smart Security periodicamente é o melhor método para se garantir o nível máximo de segurança em seu computador. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

Na janela principal do programa, ao clicar em **Atualizar**, você poderá visualizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Além das atualizações automáticas, você pode clicar em **Atualizar agora** para criar uma atualização manualmente. A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos. Dê atenção especial à sua configuração e operação. É preciso ativar seu produto usando a Chave de licença para receber atualizações. Se você não fez isso durante a instalação, você poderá inserir sua chave de licença para ativar o produto ao atualizar para acessar os servidores de atualização da ESET.

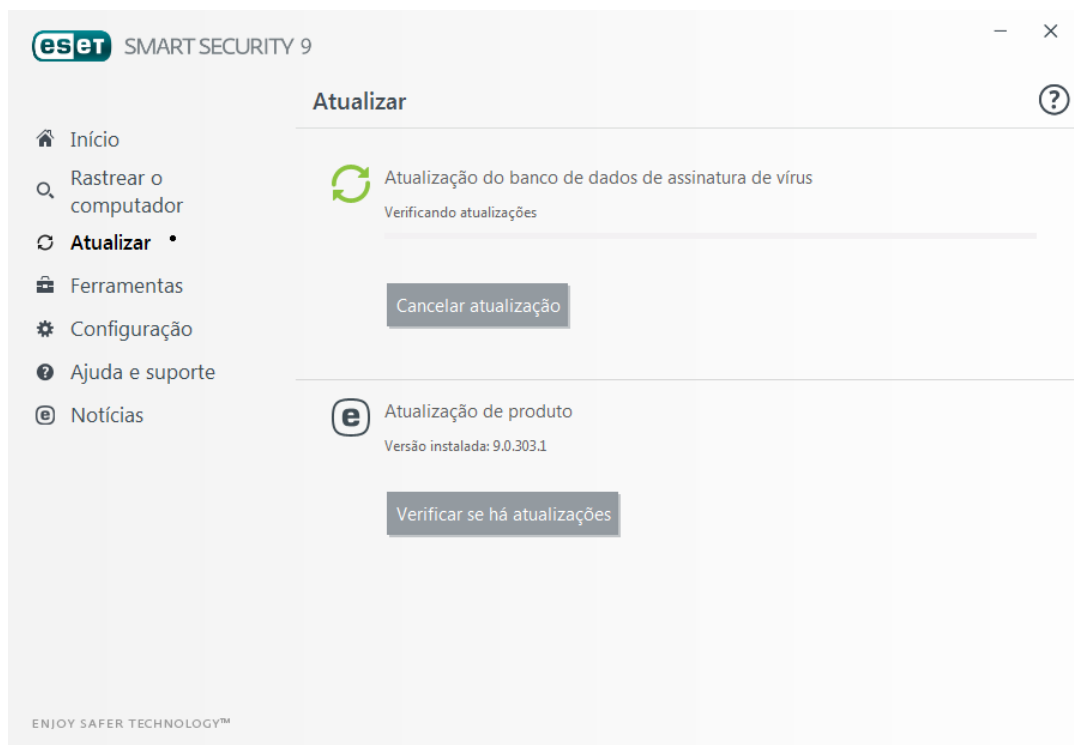
OBSERVAÇÃO: Sua chave de licença é fornecida em um email da ESET após a compra do ESET Smart Security.

Última atualização bem-sucedida - A data da última atualização. Se você não vir uma data recente,

Versão do banco de dados de assinatura de vírus – O número do banco de dados de assinatura de vírus, que também é um link ativo para o site da ESET. Clique para exibir uma lista de todas as assinaturas adicionadas em uma determinada atualização.

Clique em **Verificar atualizações** para detectar a versão disponível do ESET Smart Security mais recente.

Processo de atualização

Depois de clicar em **Atualizar agora**, o processo de download começará. A barra de progresso do download e o tempo restante do download serão exibidos. Para interromper a atualização, clique em **Cancelar atualização**.

Importante: Em circunstâncias normais, a mensagem **A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado** aparecerá na janela **Atualizar**. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize o banco de dados de assinatura de vírus assim que for possível. Caso contrário, uma das seguintes mensagens será exibida:

A notificação anterior é relacionada às duas mensagens **A atualização de banco de dados de assinatura de vírus terminou com um erro** a seguir sobre atualizações malsucedidas:

1. **Licença inválida** - A chave de licença foi inserida incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (no menu principal, clique em **Configuração** e depois em **Configuração avançada** ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Ajuda e suporte** > **Alterar licença** a partir do menu principal para inserir uma nova chave de licença.

2. **Ocorreu um erro durante o download dos arquivos de atualização** - Isso pode ser causado por Configurações de conexão com a internet incorretas. Recomendamos que você verifique a conectividade da Internet (abrindo qualquer site em seu navegador da Web). Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.

OBSERVAÇÃO: Para obter mais informações, acesse este artigo da Base de conhecimento ESET.

4.5.1 Configurações de atualização

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) em **Atualizar** > **Básico**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação sendo usados para esses servidores.

Geral

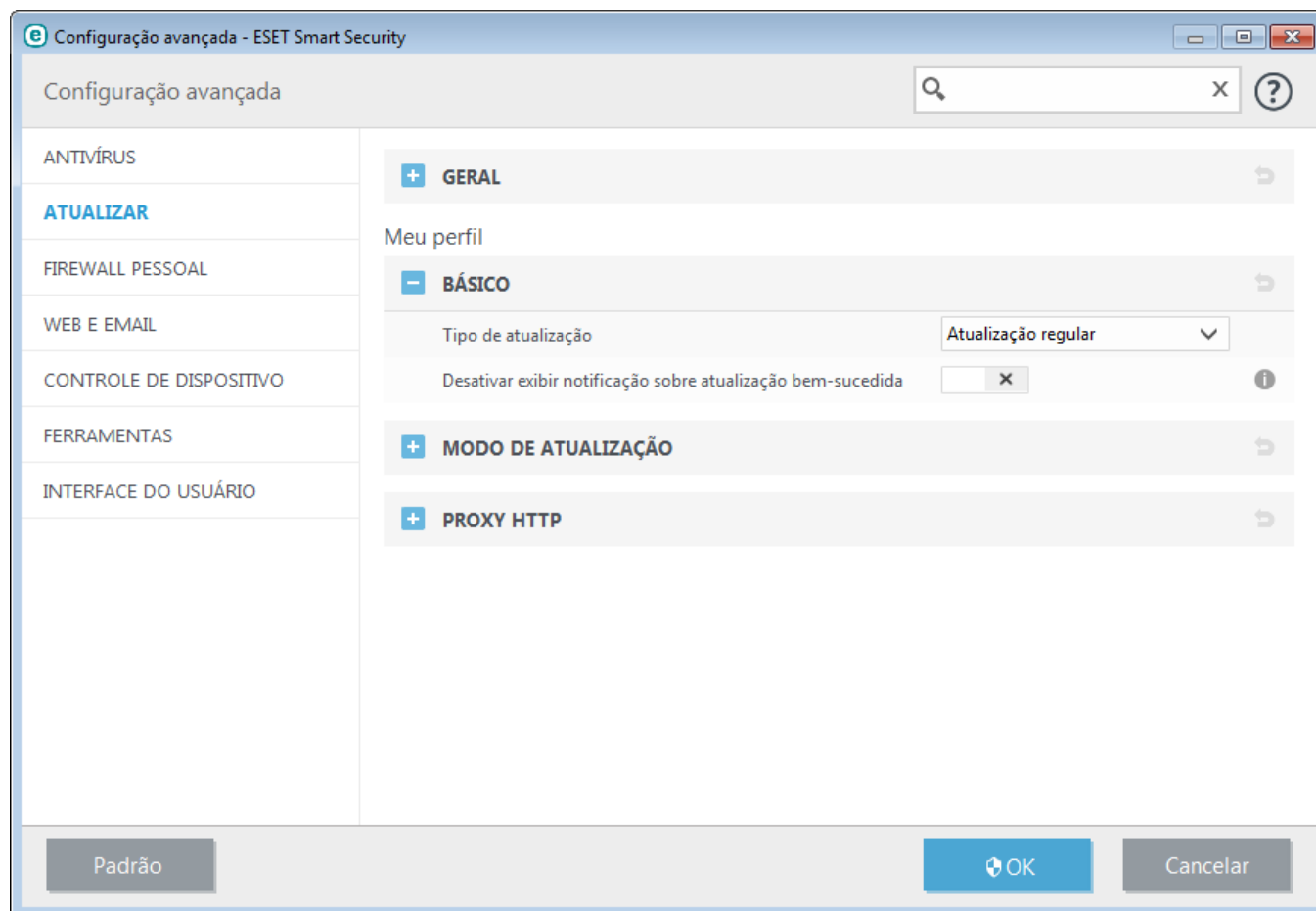
O perfil de atualização usado atualmente é exibido no menu suspenso **Perfil selecionado**. Para criar um novo perfil, clique em **Editar** ao lado de **Lista de perfis**, insira seu próprio **Nome de perfil** e então clique em **Adicionar**.

Se você está tendo dificuldade ao tentar fazer download das atualizações do banco de dados de assinatura de vírus, clique em **Limpar** para limpar os arquivos/cache de atualização temporários.

Ação disponível

Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente.

O ESET Smart Security registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de *rollback*. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar instantâneos dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Geral**), você terá que selecionar um intervalo de tempo no menu suspenso que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.

Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todos os parâmetros de atualização. Se você usar um firewall, certifique-se de que o programa da ESET tem permissão para comunicar com a Internet (por exemplo, comunicação HTTP).

Básico

Por padrão, o **Tipo de atualização** é definido como **Atualização regular** para garantir que os arquivos de atualização são obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede. Atualizações em modo de teste (a opção **Modo de teste**) são atualizações que passaram por testes internos e estarão disponíveis ao público geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável, e NÃO DEVE ser usado em servidores de produção e estações de trabalho em que é necessário ter a máxima disponibilidade e estabilidade.

Desativar exibir notificação sobre atualização bem-sucedida - Desativa a notificação da bandeja do sistema no canto inferior direito da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Lembre-se de que o Modo de apresentação desativará todas as notificações.

4.5.1.1 Atualizar perfis

Os perfis de atualização podem ser criados para várias configurações e tarefas de atualização. A criação de perfis de atualização é especialmente útil para usuários móveis, que precisam de um perfil alternativo para propriedades de conexão à Internet que mudam regularmente.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido em **Meu perfil** por padrão. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil**.

4.5.1.2 Configuração avançada de atualização

Para visualizar a Configuração avançada de atualização, clique em **Configuração...**. Opções de configuração avançada de atualização incluem a configuração de **Modo de atualização**, **Proxy HTTP** e **LAN**.

4.5.1.2.1 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa. O programa permite que você pré-defina seu comportamento quando uma nova atualização de componentes está disponível.

As atualizações de componentes do programa oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador.

Atualização de aplicativo - Quando ativado, cada atualização do componente do programa será realizada de forma automática e silenciosa, sem uma atualização completa do produto.

Se a opção **Perguntar antes de fazer download da atualização** estiver ativa, uma notificação será exibida quando uma nova atualização estiver disponível.

Se o tamanho do arquivo de atualização for maior que o valor especificado no campo **Perguntar se um arquivo de atualização for maior que (KB)**, o programa exibirá uma notificação.

4.5.1.2.2 Proxy HTTP

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore **Configuração avançada** (F5) e clique em **Proxy HTTP**. Clique no menu suspenso **Modo proxy** e selecione uma das três opções a seguir:

- Não usar servidor proxy
- Conexão através de um servidor proxy
- Usar configurações globais de servidor proxy

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Ferramentas** > **Servidor proxy** da árvore Configuração avançada.

Selecione **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Smart Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

- Deve ser usado um servidor proxy para atualizar o ESET Smart Security que seja diferente do servidor proxy especificado nas configurações globais (**Ferramentas** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação (por padrão, 3128), além do **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não foram definidas globalmente, mas o ESET Smart Security irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do Internet Explorer durante a instalação do programa; no entanto, se forem alteradas posteriormente (por exemplo, se você alterar o seu provedor de Internet), verifique se as configurações do proxy HTTP estão corretas

nesta janela. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

OBSERVAÇÃO: Os dados de autenticação, tais como **Usuário** e **Senha**, são destinados para acessar o servidor proxy. Preencha esses campos somente se um nome de usuário e uma senha forem necessários. Observe que esses campos não são para seu nome de usuário/senha do ESET Smart Security e devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

4.5.1.2.3 Conectar à rede como

Ao atualizar a partir de um servidor local com uma versão do sistema operacional Windows NT, a autenticação para cada conexão de rede é necessária por padrão.

Para configurar uma conta deste tipo, selecione a partir do menu suspenso **Tipo de usuário local**:

- **Conta do sistema (padrão)**,
- **Usuário atual**,
- **Usuário especificado**.

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

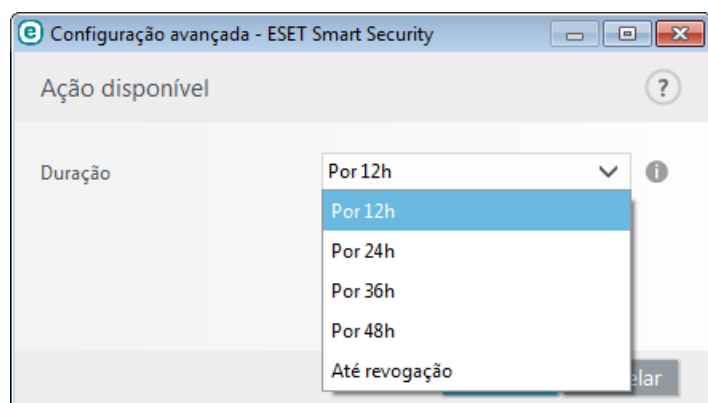
Aviso: Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: *nome_domínio\usuário* (se for um grupo de trabalho, insira o *nome_do_grupo_de_trabalho\nome*) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

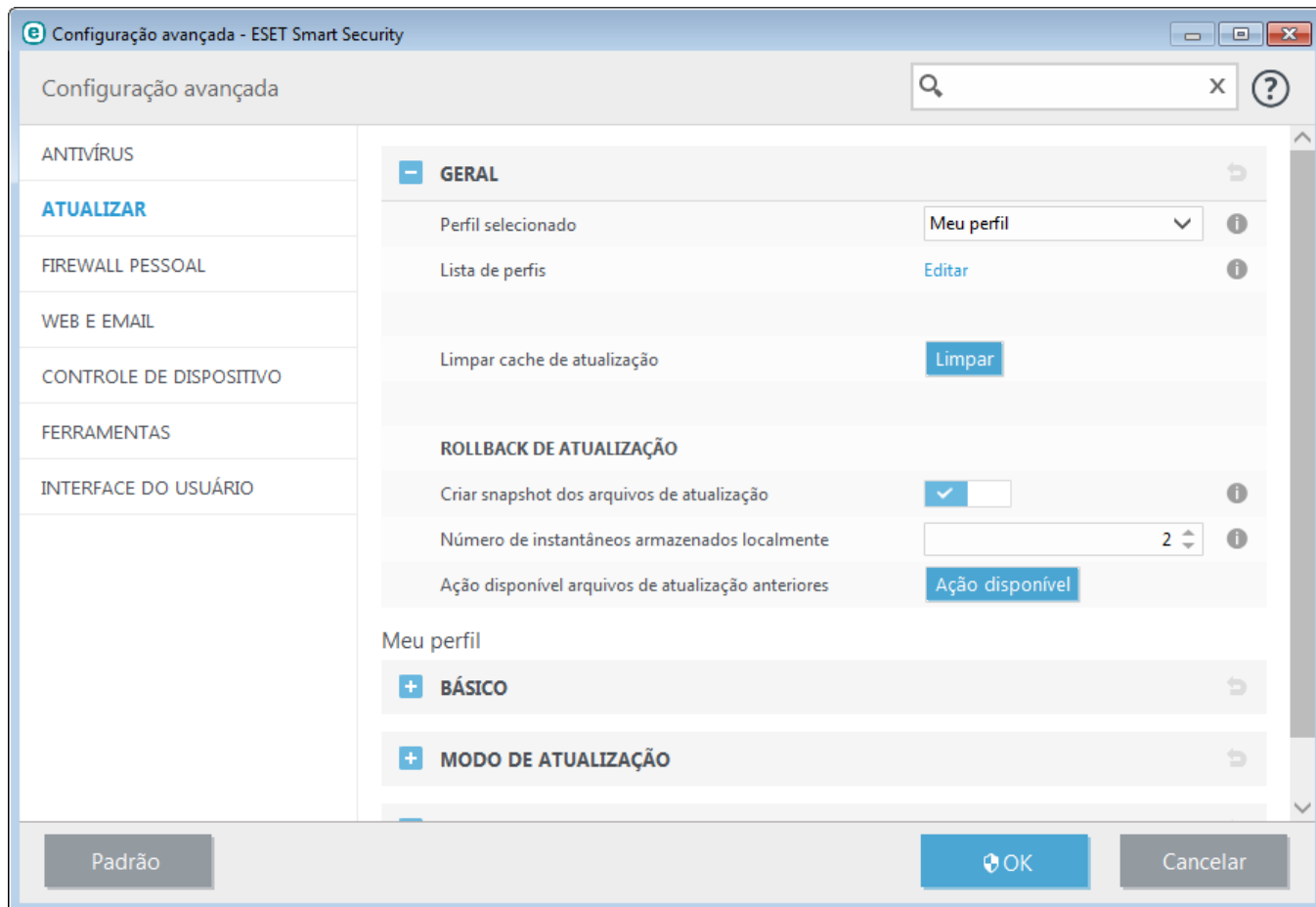
Selecione **Desconectar do servidor depois da atualização** para forçar uma desconexão se a conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

4.5.2 Rollback de atualização

Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente.

O ESET Smart Security registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de *reversão*. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar snapshots dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Atualizar reversão**), você terá que selecionar um intervalo de tempo no menu suspenso **Suspender atualizações** que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.

Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

Se um rollback for realizado, o botão **Rollback** muda para **Permitir atualizações**. Nenhuma atualização será permitida durante o intervalo de tempo selecionado no menu suspenso **Suspender atualizações**. A versão do banco de dados de assinatura de vírus é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.

Exemplo: Permita que o número 6871 seja a versão mais atual do banco de dados de assinatura de vírus. 6870 e 6868 são armazenados como instantâneos do banco de dados de assinatura de vírus. Observe que 6869 não está disponível porque, por exemplo, o computador foi desligado e uma atualização mais recente foi disponibilizada antes de a 6869 ser baixada. Se você inseriu 2 (dois) no campo **Número de instantâneos armazenados localmente** e clicou em **Reverter**, o banco de dados de assinatura de vírus (incluindo módulos do programa) será restaurado para a versão número 6868. Este processo pode demorar algum tempo. Verifique se a versão do banco de dados de assinatura de vírus foi desatualizada na janela principal do programa do ESET Smart Security na seção Atualizar.

4.5.3 Como criar tarefas de atualização

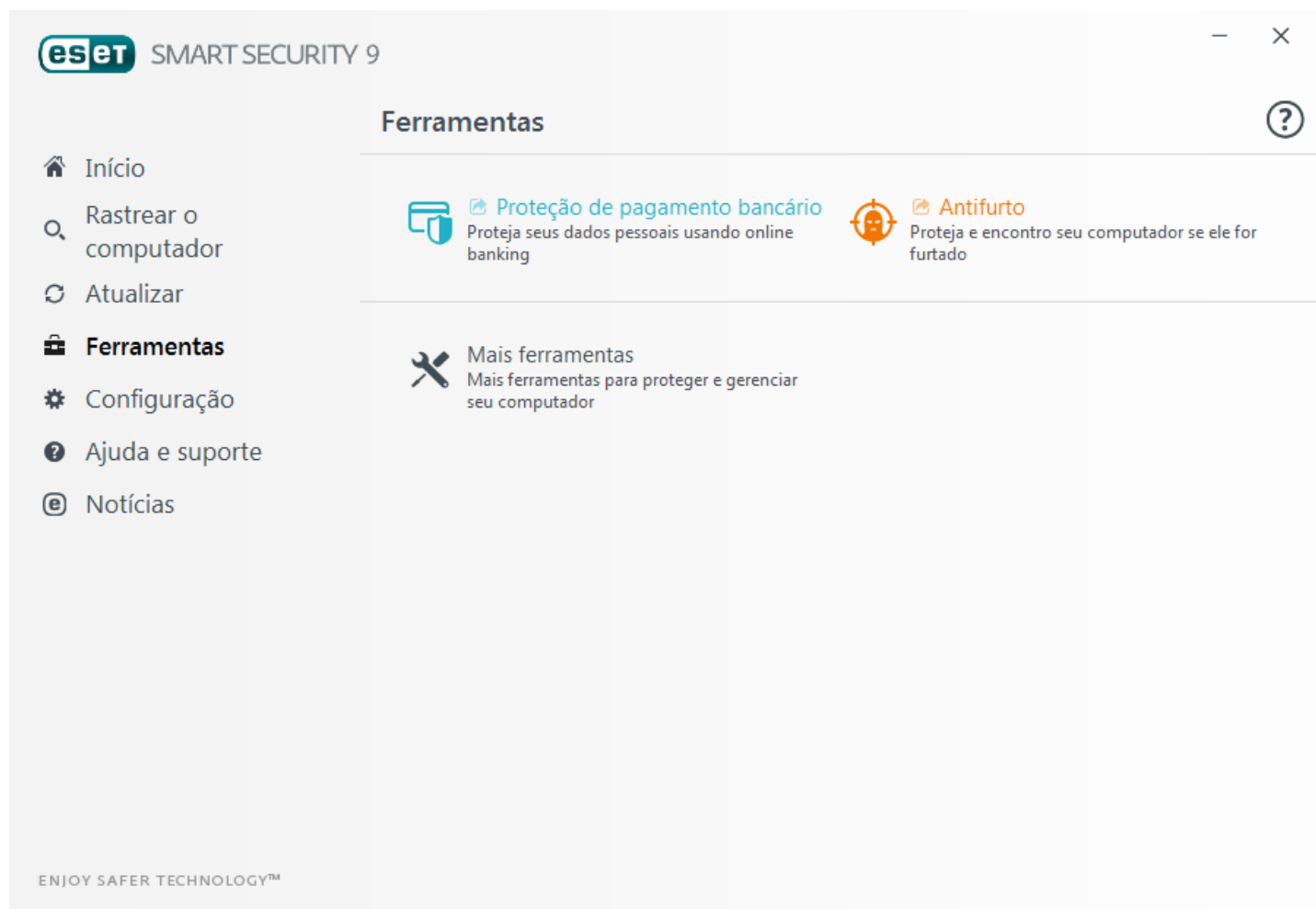
As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Smart Security:

- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**

Toda tarefa de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda.

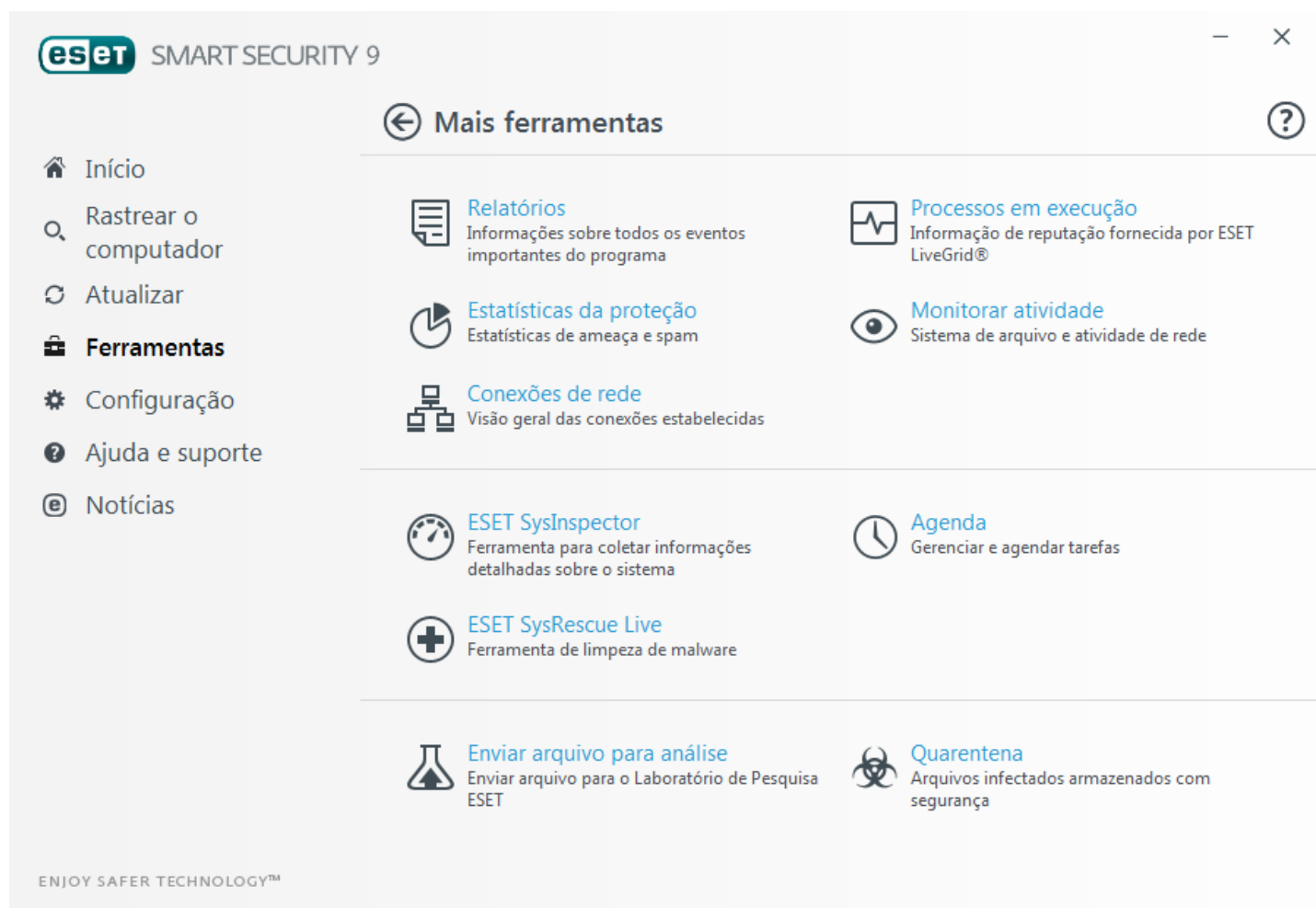
4.6 Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

Proteção para atividade bancária e pagamento - O ESET Smart Security protege os números do seu cartão de crédito e outros dados sensíveis enquanto você usa atividades bancárias on-line ou sites de pagamento. Um navegador protegido será iniciado para fornecer transações seguras de atividade bancária.

Antifurto - localiza e ajuda a encontrar seu dispositivo perdido em caso de perda ou furto.

Clique em Ferramentas no ESET Smart Security para exibir as ferramentas para proteger seu computador.

4.6.1 Ferramentas no ESET Smart Security

O **Mais ferramentas** o menu inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

Esse menu inclui as seguintes ferramentas:

Relatórios

Estatísticas da proteção

Monitorar atividade

Processos em execução (se o ThreatSense estiver ativado no ESET Smart Security)

Conexões de rede (se o Firewall pessoal estiver ativado no ESET Smart Security)

ESET SysInspector

ESET SysRescue Live - Redireciona você para a página do ESET SysRescue Live, onde é possível fazer download da imagem do ESET SysRescue Live ou Live CD/USB Creator para sistemas operacionais do Microsoft Windows.

Agenda

Enviar amostra para análise - Permite enviar um arquivo suspeito aos Laboratórios de pesquisa da ESET para análise. A janela de diálogo exibida depois de clicar nessa opção é descrita nesta seção.

Quarentena

OBSERVAÇÃO: O ESET SysRescue pode não estar disponível para Windows 8 em versões anteriores de produtos de segurança ESET. Nesse caso recomendamos que você atualize seu produto ou crie um disco ESET SysRescue em outra versão do Microsoft Windows.

4.6.1.1 Arquivos de log

Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log é uma parte essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do log. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET Smart Security, bem como arquivar logs.

Os relatórios podem ser acessados na janela principal do programa, clicando em **Ferramentas** > **Mais ferramentas** > **Relatórios**. Selecione o tipo de log desejado no menu suspenso **Log** Os seguintes logs estão disponíveis:

- **Ameaças detectadas** - O log de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelo ESET Smart Security. As informações de relatório incluem a hora da detecção, nome da ameaça, local, ação realizada e o nome do usuário conectado no momento em que a ameaça foi detectada. Clique duas vezes em qualquer entrada de log para exibir seus detalhes em uma janela separada.
- **Eventos** - Todas as ações importantes executadas pelo ESET Smart Security são registradas no log de eventos. O log de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para a solução de problemas de administradores do sistema e de usuários. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.
- **Rastrear o computador** - Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo rastreamento.
- **HIPS** - Contém registros de regras específicas de HIPS que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.
- **Firewall pessoal** - O log do firewall exibe todos os ataques remotos detectados pelo firewall pessoal. Aqui, você vai encontrar informações sobre todos os ataques em seu computador. A coluna *Evento* lista os ataques detectados. A coluna *Origem* informa mais sobre quem atacou. A coluna *Protocolo* revela o protocolo de comunicação usado para o ataque. A análise do log do firewall pode ajudá-lo a detectar tentativas de infiltração do sistema a tempo de evitar o acesso sem autorização ao sistema.
- **Sites filtrados** - Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela Proteção de acesso à web ou Controle dos pais. Nesses relatórios você poderá ver o horário, endereço URL, usuário e aplicativo que criaram uma conexão para o site específico.
- **Proteção antispam** - Contém registros relacionados com emails marcados como spam.
- **Controle dos pais** - Mostra páginas da web bloqueadas ou permitidas pelo Controle dos pais. As colunas *Tipo de correspondência* e *Valores de correspondência* mostram como as regras de filtragem foram aplicadas.
- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com Regras de controle de dispositivo respectivas serão registrados no arquivo de log. Se a regra não coincidir com um dispositivo conectado, uma entrada de log para um dispositivo conectado não será criada. Aqui, você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).

Em cada seção, as informações exibidas podem ser copiadas para a área de transferência selecionando e usando o atalho de teclado **Ctrl + C**. Para selecionar várias entradas, as teclas **Ctrl** e **Shift** podem ser usadas.

Clique em **Filtragem** para abrir a janela **Filtragem de relatórios** onde poderá definir os critérios de filtragem.

Você pode exibir o menu de contexto clicando com o botão direito em um registro específico. As seguintes opções também estão disponíveis no menu de contexto.

- **Mostrar** - Mostra informações mais detalhadas sobre o relatório selecionado em uma nova janela.
- **Filtrar registros do mesmo tipo** - Depois de ativar esse filtro, você só verá registros do mesmo tipo (diagnósticos, avisos...).
- **Filtrar.../Localizar...** - Depois de clicar nessa opção, a janela Pesquisar no relatório permitirá que você defina critérios de filtragem para entradas de relatório específicas.
- **Ativar filtro** - Ativa configurações de filtro.
- **Desativar filtro** - Apaga todas as configurações do filtro (conforme descrição acima).
- **Copiar/Copiar tudo** - Copia informações sobre todos os registros na janela.
- **Excluir/Excluir tudo** - Exclui o(s) registro(s) selecionado(s) ou todos os exibidos - essa ação requer privilégios de administrador.
- **Exportar...** - Exporta informações sobre o(s) registro(s) em formato XML.
- **Exportar todos...** - Exporta informações sobre todos os registros em formato XML.
- **Percorrer relatório** - Deixe esta opção ativada para percorrer automaticamente relatórios antigos e monitorar relatórios ativos na janela **Relatórios**.

4.6.1.1.1 Relatórios

A configuração de logs do ESET Smart Security pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Arquivos de log**. A seção de logs é utilizada para definir como os logs serão gerenciados. O programa exclui automaticamente os logs mais antigos a fim de economizar espaço no disco rígido. Você pode especificar as seguintes opções para logs:

Detalhamento mínimo de registro em log - Especifica o nível de detalhamento mínimo de eventos a serem registrados em log.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como *"Erro ao fazer download de arquivo"* e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, a firewall pessoal, etc...).

As entradas de relatório anteriores ao número de dias especificado no campo **Excluir registros anteriores a (dias)** são automaticamente excluídas.

Otimizar automaticamente arquivos de log - Se selecionada, os arquivos de log serão automaticamente desfragmentados se a porcentagem for superior ao valor especificado no campo **Se o número de registros não utilizados excede (%)**.

Clique em **Otimizar** para começar a desfragmentar os relatórios. Todas as entradas de logs vazias são removidas durante esse processo, o que melhora o desempenho e a velocidade de processamento de logs. Essa melhoria pode ser observada especialmente se os logs tiverem um grande número de entradas.

Ativar protocolo de texto permite a armazenagem de relatórios em outro formato de arquivo, separado dos Relatórios:

- **Diretório de destino** - O diretório no qual relatórios serão armazenados (aplica-se somente a texto/CSV). Cada seção do relatório tem seu próprio arquivo com um nome de arquivo predefinido (por exemplo, *virlog.txt* para a seção **Ameaças detectadas** dos relatórios, se você usar formato de arquivo de texto simples para armazenar relatórios).

- **Tipo** - Se você selecionar o formato de arquivo **Texto**, os relatórios serão armazenados em um arquivo de texto, os dados serão separados por tabulações. O mesmo se aplica a formato de arquivo **CSV** separado por vírgulas. Se você escolher **Evento**, os relatórios serão armazenados no relatório de eventos do Windows (pode ser visualizado usando o Visualizador de eventos no Painel de controle) ao contrário do arquivo.

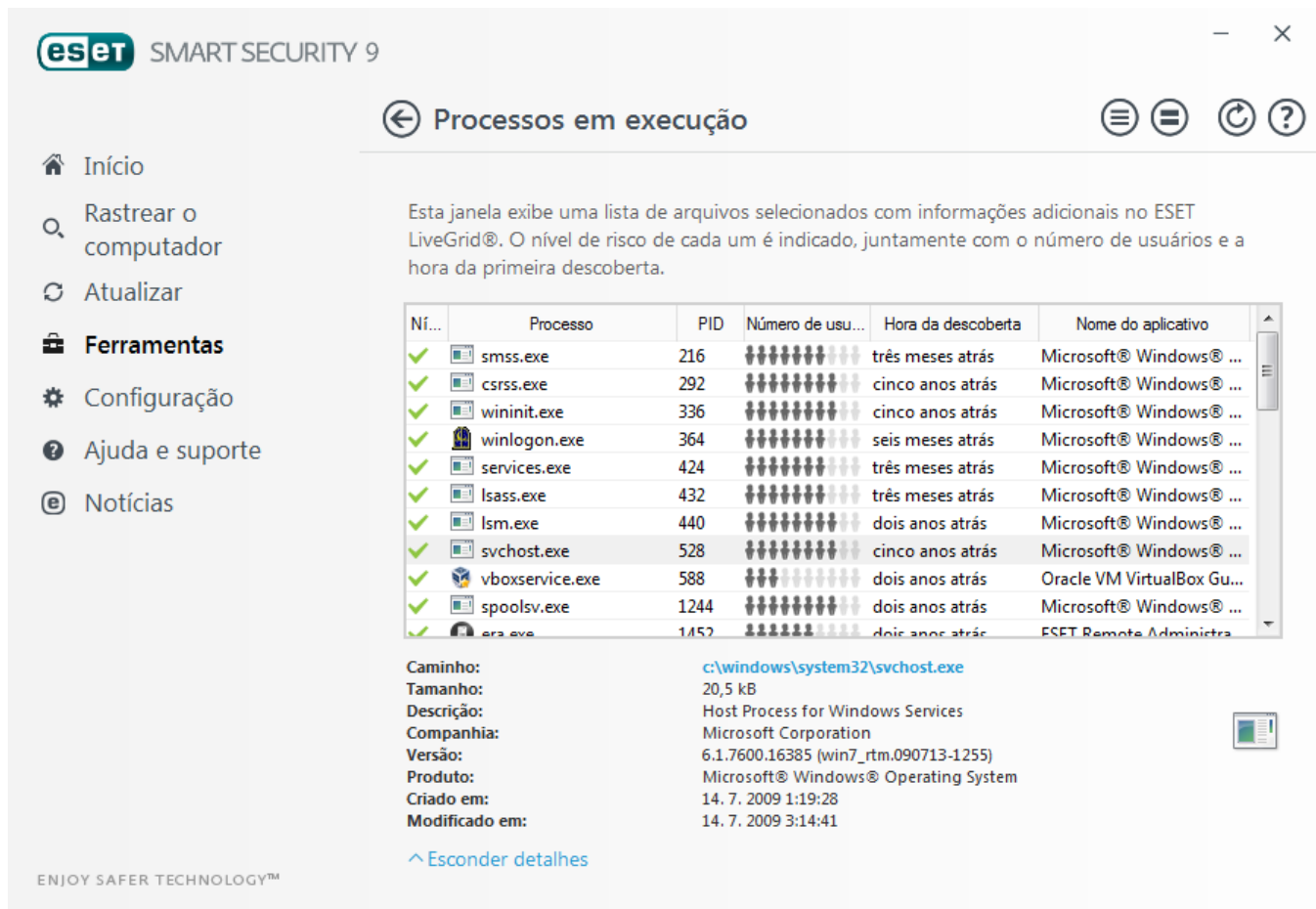
Excluir todos os relatórios - Apaga todos os relatórios armazenados atualmente selecionados no menu suspenso

Tipo. Uma notificação sobre a exclusão bem sucedida dos relatórios será exibida.

OBSERVAÇÃO: Para ajudar a resolver problemas mais rapidamente, a ESET poderá solicitar que você forneça relatórios de seu computador. O Coletor de Relatório ESET facilita sua coleta das informações necessárias. Para obter mais informações sobre o Coletor de relatório ESET, consulte nosso artigo da Base de conhecimento ESET.

4.6.1.1.2 Microsoft NAP

A Proteção do acesso à rede (NAP) é uma tecnologia da Microsoft para controlar o acesso à rede de um computador host com base na integridade do sistema do host. Com a NAP, os administradores de sistema da rede de computadores de uma empresa podem definir políticas para os requisitos de integridade do sistema.

O NAP (Network Access Protection, Proteção de acesso à rede) foi desenvolvido para ajudar os administradores a manter a integridade dos computadores da rede, que por sua vez ajuda a manter a integridade geral da rede. Ele não foi desenvolvido para proteger uma rede de usuários mal-intencionados. Por exemplo, se um computador tiver todo o software e configurações que a política de acesso à rede requer, o computador será considerado íntegro ou em conformidade e o acesso apropriado à rede será concedido. O NAP não impede que um usuário autorizado com um computador em conformidade carregue um programa malicioso na rede ou se envolva em outro comportamento indevido.

O NAP permite que os administradores criem e apliquem políticas de integridade para computadores que se conectem à rede corporativa. As políticas regem os componentes de software instalados e as configurações do sistema. Os computadores conectados à rede, como laptops, estações de trabalho e outros dispositivos semelhantes, são avaliados em relação aos requisitos de integridade configurados.

Entre os requisitos de integridade estão:

- Um firewall está ativado,
- Um programa antivírus está instalado,
- O programa antivírus está atualizado,
- As atualizações automáticas do Windows estão ativadas, etc.

4.6.1.2 Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET Smart Security oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia ThreatSense.

Processo - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção **Gerenciador de tarefas** ou pressionando Ctrl+Shift+Esc no teclado.

Nível de risco - Na maioria dos casos, o ESET Smart Security e a tecnologia ThreatSense atribui níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 – Aceitável (verde) a 9 – Perigoso (vermelho).

OBSERVAÇÃO: Aplicativos conhecidos marcados como Aceitável (verde) são limpos definitivamente (lista de permissões) e serão excluídos do rastreamento, pois isso melhorará a velocidade do rastreamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

Número de usuários - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ThreatSense.

Hora da descoberta - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ThreatSense.

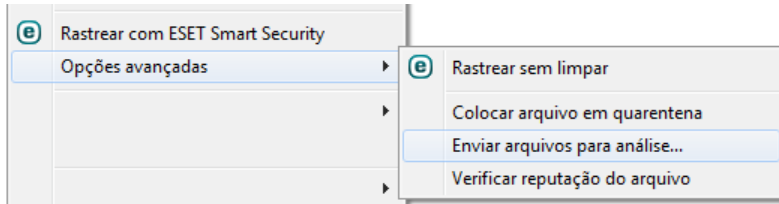
OBSERVAÇÃO: Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se você não estiver certo em relação ao arquivo, poderá enviar o arquivo para análise ao Laboratório pesquisa da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Nome do aplicativo - O nome de um programa ou processo.

Abrir em uma nova janela - As informações dos processos em execução serão abertas em uma nova janela.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

- **Arquivo** - Local de um aplicativo no computador.
- **Tamanho do arquivo** - Tamanho do arquivo em B (bytes).
- **Descrição do arquivo** - Características do arquivo com base na descrição do sistema operacional.
- **Nome da empresa** - Nome de processo do aplicativo ou do fornecedor.
- **Versão do arquivo** - Informações do editor do aplicativo.
- **Nome do produto** - Nome do aplicativo e/ou nome comercial.

OBSERVAÇÃO: A reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e selecione **Opções avançadas** > **Verificar reputação do arquivo usando o ThreatSense**.

4.6.1.3 Estatísticas da proteção

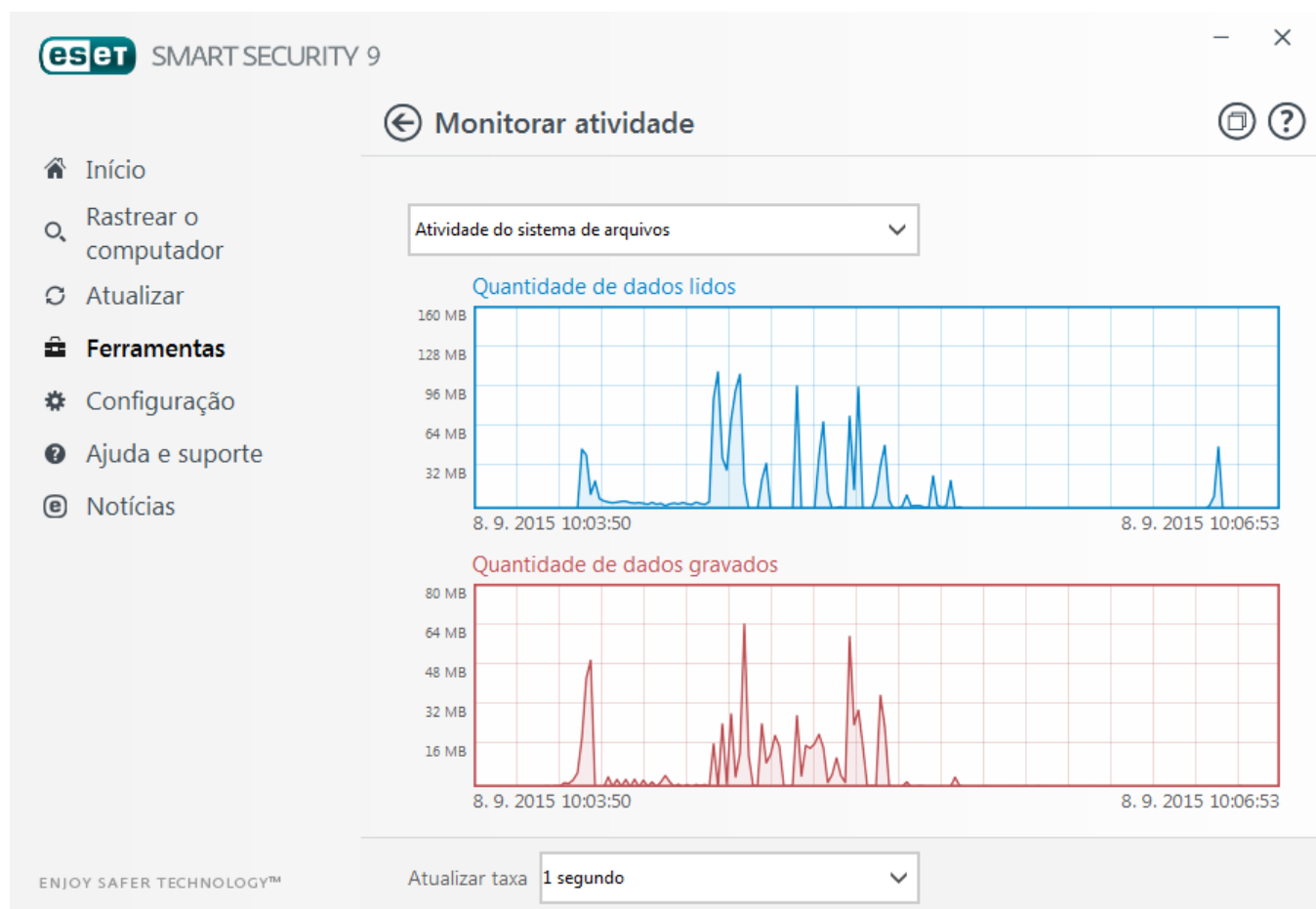
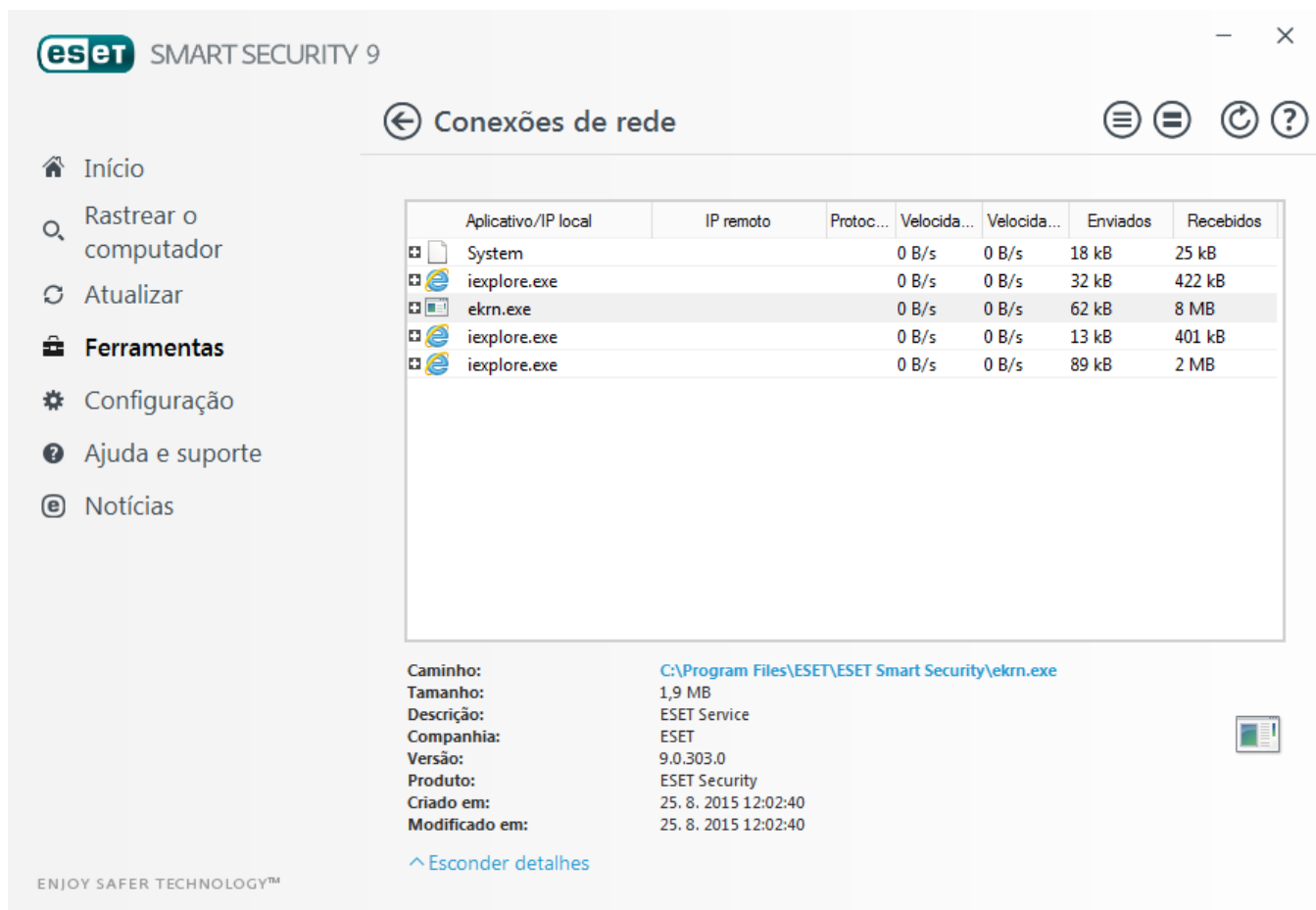
Para exibir um gráfico de dados estatísticos relacionados aos módulos de proteção do ESET Smart Security, clique em **Ferramentas** > **Estatísticas da proteção**. Selecione o módulo de proteção desejado no menu suspenso **Estatísticas** para visualizar o gráfico e a legenda correspondentes. Se você passar o mouse sobre um item na legenda, somente os dados desse item serão exibidos no gráfico.

Os gráficos estatísticos a seguir estão disponíveis:

- **Proteção antifírus e antispyware** - Exibe o número de objetos infectados e limpos.
- **Proteção do sistema de arquivos** - Exibe apenas os objetos que foram lidos ou gravados no sistema de arquivos.
- **Proteção do cliente de email** - Exibe apenas os objetos que foram enviados ou recebidos pelos clientes de email.
- **Proteção antiphishing e de acesso à Web** - Exibe apenas os objetos obtidos por download pelos navegadores da web.
- **Proteção antispam do cliente de email** - Exibe o histórico das estatísticas de antispam desde a última inicialização.

Abaixo dos gráficos de estatísticas, você pode ver o número total de objetos rastreados, o último objeto rastreado e o registro de estatísticas. Clique em **Redefinir** para apagar todas as informações estatísticas.

4.6.1.4 Monitorar atividade

Para visualizar a **Atividade do sistema de arquivos** atual em forma gráfica, clique em **Ferramentas** > **Mais ferramentas** > **Monitorar atividade**. Na parte inferior do gráfico, há uma linha do tempo que grava a atividade do sistema de arquivos em tempo real com base na duração do tempo selecionado. Para alterar a duração do tempo, selecione a partir do menu suspenso **Atualizar taxa**.

As opções disponíveis são:

- **Etapa: 1 segundo** - O gráfico é atualizado a cada segundo e a linha de tempo cobre os últimos 10 minutos.
- **Etapa: 1 minuto (últimas 24 horas)** - O gráfico é atualizado a cada minuto e a linha de tempo cobre as últimas 24 horas.
- **Etapa: 1 hora (último mês)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês.
- **Etapa: 1 hora (mês selecionado)** - O gráfico é atualizado a cada hora e a linha de tempo cobre os últimos X meses selecionados.

O eixo vertical do **Gráfico da atividade do sistema de arquivos** representa os dados lidos (azul) e os dados gravados (vermelho). Ambos os valores são fornecidos em KB (kilobytes)/MB/GB. Se você passar o mouse sobre os dados lidos ou sobre os dados gravados na legenda embaixo do gráfico, apenas os dados para esse tipo de atividade serão exibidos no gráfico.

Você também pode selecionar **Atividade de rede** a partir do menu suspenso **Atividade**. A exibição do gráfico e as opções da **Atividade do sistema de arquivos** e da **Atividade de rede** são as mesmas, exceto que a última exibe os dados recebidos (vermelho) e os dados enviados (azul).

4.6.1.5 Conexões de rede

Na seção Conexões de rede, você pode ver uma lista de conexões ativas e pendentes. Isso o ajuda a controlar todos os aplicativos que estabelecem conexões de saída.

A primeira linha exibe o nome do aplicativo e a velocidade de transferência dos dados. Para ver a lista de conexões feitas pelo aplicativo (bem como informações mais detalhadas), clique em **+**.

Colunas

Aplicativo/IP local - Nome do aplicativo, endereços IP locais e portas de comunicação.

IP remoto - Endereço IP e número de porta de um computador remoto específico.

Protocolo - Protocolo de transferência utilizado.

Velocidade de entrada/de saída - A velocidade atual dos dados de saída e entrada.

Enviados/Recebidos - Quantidade de dados trocados na conexão.

Mostrar detalhes - Escolha esta opção para exibir informações detalhadas sobre a conexão selecionada.

A opção **Configuração de visualização da conexão...** na tela Conexões de rede insere a estrutura de configuração avançada para esta seção, permitindo a modificação das opções de exibição da conexão:

Solucionar nomes de host - Se possível, todos os endereços de rede serão exibidos no formato DNS, não no formato de endereço IP numérico.

Exibir somente conexões TCP - A lista só exibe conexões que pertencem ao pacote de protocolo TCP.

Mostrar conexões de escuta - Selecione essa opção para exibir somente conexões em que não haja comunicação atualmente estabelecida, mas o sistema tenha aberto uma porta e esteja aguardando por conexão.

Mostrar conexões no computador - Selecione essa opção para mostrar somente conexões nas quais o lado remoto é um sistema local - as chamadas conexões de *localhost*.

Clique com o botão direito do mouse em uma conexão para visualizar as opções adicionais, que incluem:

Negar comunicação para a conexão - Encerra a comunicação estabelecida. Essa opção só fica disponível depois que você clica em uma conexão ativa.

Velocidade de atualização - Escolha a frequência para atualizar as conexões ativas.

Atualizar agora - Recarrega a janela Conexões de rede.

As opções a seguir só ficam disponíveis depois que você clica em um aplicativo ou processo, não em uma conexão ativa:

Negar temporariamente comunicação para o processo - Rejeita as atuais conexões de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Configuração e uso de regras.

Permitir temporariamente comunicação para o processo - Permite as conexões atuais de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Configuração e uso de regras.

4.6.1.6 ESET SysInspector

o ESET SysInspector é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos instalados, as conexões de rede ou entradas de registo importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware.

A janela do SysInspector exibe as seguintes informações sobre os logs criados:

- **Hora** - A hora de criação do log.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o log.
- **Status** - O status de criação do log.

As seguintes ações estão disponíveis:

- **Abrir** - Abre um relatório criado. Também é possível clicar com o botão direito do mouse em um determinado relatório e selecionar **Exibir** no menu de contexto.
- **Comparar** - Compara dois logs existentes.
- **Criar...** - Cria um novo log. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como Criado) antes de tentar acessar o relatório.
- **Excluir** - Exclui os relatórios selecionados da lista.

Os itens a seguir estão disponíveis no menu de contexto quando um ou mais relatórios são selecionados:

- **Mostrar** - Abre o log selecionado no ESET SysInspector (igual a clicar duas vezes em um log).
- **Comparar** - Compara dois relatórios existentes.
- **Criar...** - Cria um novo relatório. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como Criado) antes de tentar acessar o relatório.
- **Excluir tudo** - Exclui todos os logs.
- **Exportar...** - Exporta o log para um arquivo *.xml* ou *.xml* compactado.

4.6.1.7 Agenda

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas.

A Agenda pode ser acessada na janela principal do programa do ESET Smart Security em **Ferramentas** > **Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

O Agendador serve para agendar as seguintes tarefas: atualização do banco de dados das assinaturas de vírus, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do log. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar...** ou **Excluir** na parte inferior). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa e excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção de logs**
- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**
- **Verificação regular pela última versão do produto** (consulte Modo de atualização)
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após atualização bem sucedida do banco de dados de assinatura de vírus)
- **Primeiro rastreamento automático**

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

Adicionar uma nova tarefa

1. Clique em **Adicionar tarefa** na parte inferior da janela.

2. Insira um nome da tarefa.

3. Selecione a tarefa desejada no menu suspenso:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de relatório** - Os relatórios também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de relatório para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um rastreamento do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - Por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

4. Ative a opção **Ativado** se quiser ativar a tarefa (você pode fazer isso posteriormente marcando/desmarcando a caixa de seleção na lista de tarefas agendadas), clique em **Avançar** e selecione uma das opções de tempo:

- **Uma vez** - A tarefa será realizada na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
- **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
- **Semanalmente** - A tarefa será realizada na data e hora selecionadas.
- **Evento disparado** - A tarefa será realizada após um evento especificado.

5. Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Você pode revisar a tarefa agendada clicando com o botão direito do mouse em **Mostrar detalhes da tarefa**.

4.6.1.8 ESET SysRescue

o ESET SysRescue é um utilitário que permite criar um disco inicializável que contém uma das soluções ESET Security - ESET NOD32 Antivirus, ESET Smart Security ou certos produtos feitos para servidor. A principal vantagem do ESET SysRescue é o fato de a solução ESET Security ser executada de maneira independente do sistema operacional host, mas tem um acesso direto ao disco e ao sistema de arquivos. Isso possibilita remover as infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

4.6.1.9 ESET LiveGrid®

ESET LiveGrid® (construído sobre o sistema de alerta precoce avançado ThreatSense.Net) usa dados que os usuários ESET enviaram em todo o mundo e envia-os para o Laboratório de pesquisa ESET. Ao fornecer amostras suspeitas e metadados originais, o ESET LiveGrid® nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes. Leia mais sobre o ESET LiveGrid® no glossário.

O usuário pode verificar a reputação dos arquivos e dos processos em execução diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET LiveGrid®. Há duas opções:

1. Você pode escolher não ativar o ESET LiveGrid®. Você não perderá nenhuma funcionalidade do software, mas, em alguns casos, o ESET Smart Security poderá responder mais rápido a novas ameaças do que a atualização do banco de dados de assinatura de vírus quando o ESET Live Grid estiver ativado.
2. É possível configurar o ESET LiveGrid® para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ESET LiveGrid® coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET Smart Security é configurado para enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como *.doc* ou *.xls*, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

O menu de configuração do ESET LiveGrid® fornece várias opções para ativar/desativar o ESET LiveGrid®, que serve para enviar arquivos suspeitos e informações estatísticas anônimas para os laboratórios da ESET. Ele pode ser acessado a partir da árvore Configuração avançada clicando em **Ferramentas** > **ESET LiveGrid®**.

Ativar o sistema de reputação ESET LiveGrid® (recomendado) - O sistema de reputação do ESET LiveGrid® melhora a eficiência de soluções anti-malware da ESET ao comparar os arquivos rastreados com um banco de dados de itens na lista de proibições e permissões da nuvem.

Enviar estatísticas anônimas - Permite que a ESET colete informações sobre ameaças recém-detectadas como o nome, data e hora de detecção da ameaça, método de detecção e metadados associados, versão e configuração do produto, inclusive informações sobre seu sistema.

Enviar arquivos - Arquivos suspeitos, que se pareçam com ameaças e/ou arquivos com características ou comportamento incomuns são enviados à ESET para análise.

Selecione **Ativar registro em relatório** para criar um relatório de eventos para registrar os envios de arquivos e informações estatísticas. Isso vai permitir o registro no Relatório de eventos quando as estatísticas ou os arquivos são enviados.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Exclusão - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Se já tiver usado o ESET LiveGrid® antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET. Assim que todas as informações atuais forem enviadas, não serão criados pacotes adicionais.

4.6.1.9.1 Arquivos suspeitos

A guia **Arquivos** na configuração avançada do ESET LiveGrid® permite configurar como as ameaças serão enviadas ao Laboratório de vírus da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de pesquisa ESET. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

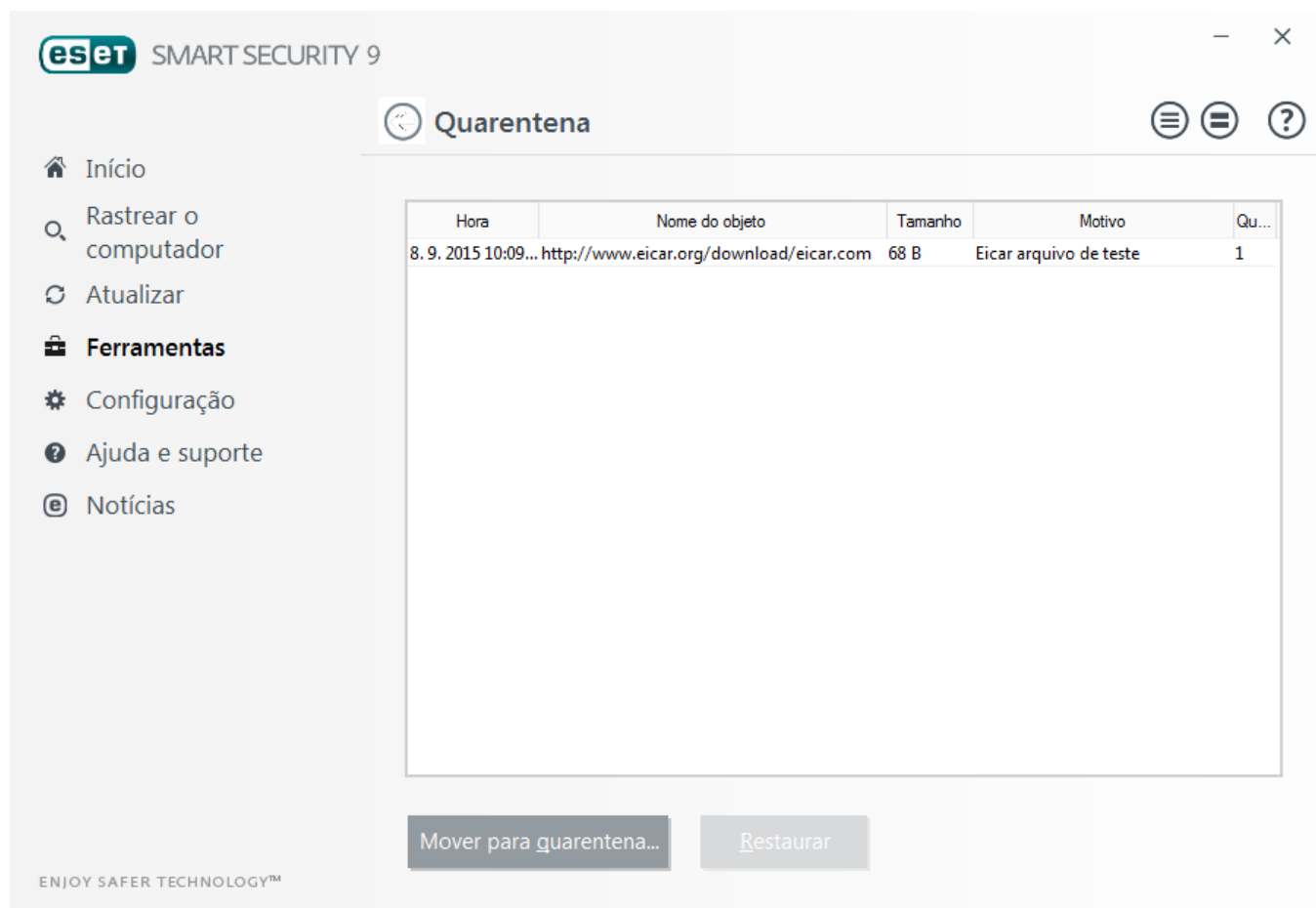
Filtro de exclusões - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Os arquivos relacionados nunca serão enviados aos laboratórios de pesquisa da ESET para análise, mesmo se incluírem um código suspeito. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Selecione **Ativar registro em log** para criar um log de eventos para registrar os envios de arquivos e informações estatísticas. Isso vai permitir o registro no Log de eventos quando as estatísticas ou os arquivos são enviados.

4.6.1.10 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Smart Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de pesquisa da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

Colocação de arquivos em quarentena

O ESET Smart Security coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena...**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena...**

Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Utilize o recurso **Restaurar** para essa finalidade, que está disponível no menu de contexto clicando com o botão direito do mouse no arquivo desejado, na janela Quarentena. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, **Restaurar e excluir do rastreamento** será ativado. Leia mais sobre esse tipo de aplicativo no glossário. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO: se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do

rastreamento após restaurá-lo e envie-o para o Atendimento ao Cliente da ESET.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.6.1.11 Servidor proxy

Em grandes redes LAN, a comunicação entre seu computador e a Internet pode ser mediada por um servidor proxy. Usando esta configuração, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não poderá se atualizar automaticamente. No ESET Smart Security, a configuração do servidor proxy está disponível a partir de duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Smart Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

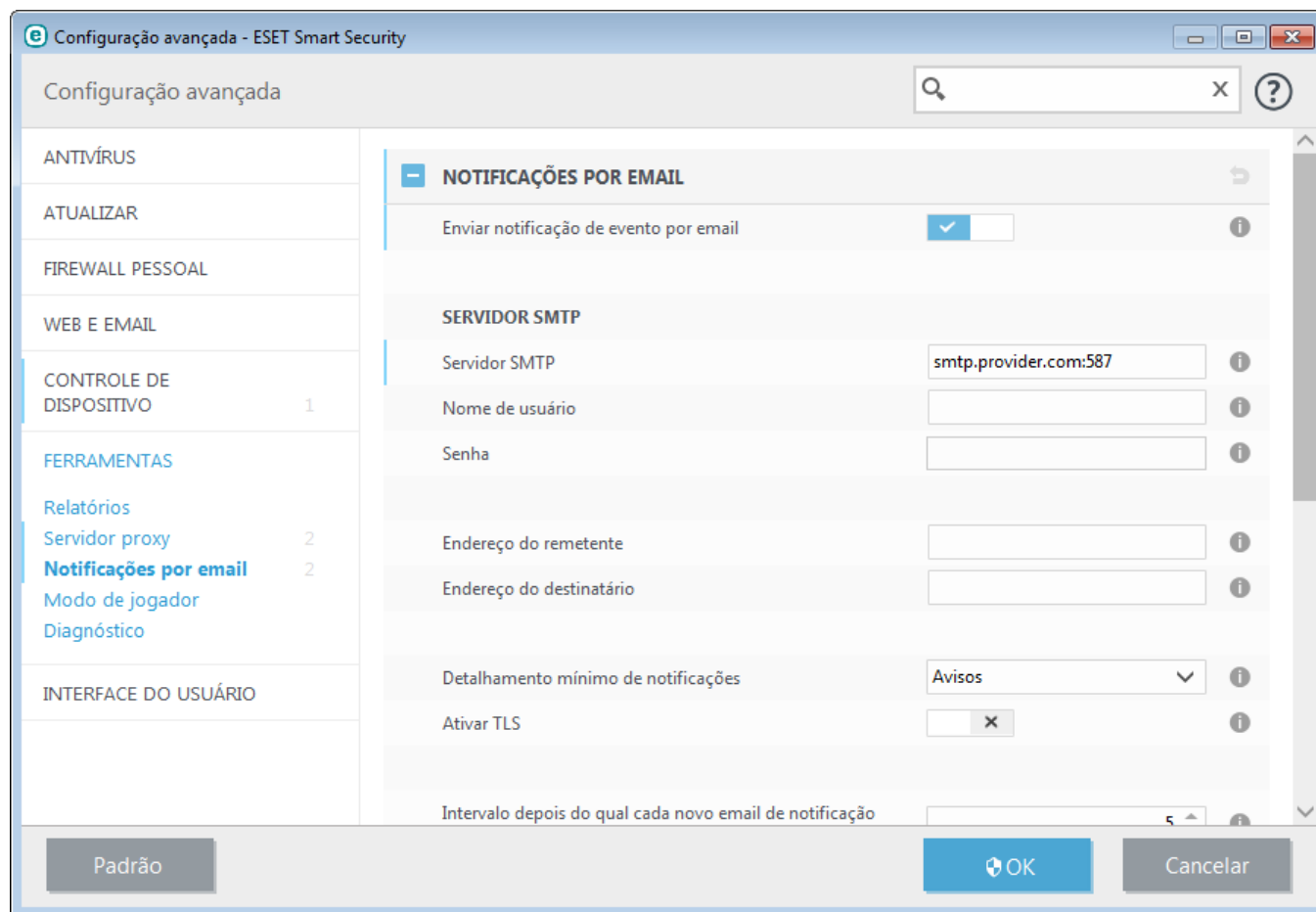
Para especificar as configurações do servidor proxy para esse nível, selecione **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, selecione **O servidor proxy requer autenticação** e digite um **Nome de usuário** e uma **Senha** válidos nos respectivos campos. Clique em **Detectar** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

OBSERVAÇÃO: É preciso inserir manualmente seu Nome de usuário e Senha nas configurações do **Servidor proxy**.

Configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (**Configuração avançada**> **Atualizar** > **Proxy HTTP** ao selecionar **Conexão através de um servidor proxy** no menu suspenso **Modo proxy**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações de assinatura de vírus de locais remotos. Para obter mais informações sobre essa configuração, consulte Configuração avançada de atualização.

4.6.1.12 Notificações por email

O ESET Smart Security poderá enviar automaticamente e-mails de notificação se um evento com o nível de detalhamento selecionado ocorrer. Ative **Enviar notificações de evento por email** para ativar notificações por e-mail.

Servidor SMTP

Servidor SMTP - O servidor SMTP usado para o envio de notificações. (por exemplo *smtp.provider.com:587*, a porta pré-definida é 25).

OBSERVAÇÃO: Os servidores SMTP com criptografia TLS são compatíveis com o ESET Smart Security.

Nome de usuário e **senha** - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos para conceder acesso ao servidor SMTP.

Endereço do remetente - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos emails de notificação.

Endereço do destinatário - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação.

No menu suspenso **Detalhamento mínimo de notificações**, é possível selecionar o nível de gravidade inicial das notificações a serem enviadas.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas como eventos de rede fora do padrão, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso (o Anti-Stealth não está sendo executado corretamente ou a atualização falhou).
- **Erros** - Erros (proteção de documentos não iniciada) e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos como erro ao iniciar a proteção antivírus ou sistema infectado.

Ativar TLS - Ativa o envio de mensagens de alerta e notificação compatíveis com a criptografia TLS.

Intervalo depois do qual cada novo email de notificação será enviado (min) - Intervalo em minutos depois do qual cada nova notificação será enviada por email. Se configurar este valor como 0, as notificações serão enviadas imediatamente.

Enviar cada notificação em um email separado - Quando ativado, o destinatário receberá um novo email para cada notificação individual. Isso pode resultar em um grande número de emails recebidos em um curto período de tempo.

Formato de mensagem

Formato de mensagens de eventos - O formato de mensagens de eventos que são exibidas em computadores remotos.

Formato das mensagens de aviso de ameaça - Mensagens de alerta de ameaça e notificação têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

Utilizar caracteres do alfabeto local - Converte uma mensagem de email na codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").

Utilizar codificações de caracteres locais - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

4.6.1.12.1 Formato de mensagem

Aqui é possível configurar o formato das mensagens de eventos que são exibidas em computadores remotos.

As mensagens de alerta e notificação de ameaças têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

As palavras-chave (cadeias de caractere separadas por sinais %) são substituídas na mensagem pelas informações reais conforme especificadas. As palavras-chave disponíveis são:

- **%TimeStamp%** - Data e hora do evento
- **%Scanner%** - Módulo relacionado
- **%ComputerName%** - Nome do computador no qual o alerta ocorreu
- **%ProgramName%** - Programa que gerou o alerta
- **%InfectedObject%** – Nome do arquivo, mensagem, etc. infectados
- **%VirusName%** - Identificação da infecção
- **%ErrorDescription%** -Descrição de um evento não vírus

As palavras-chave **%InfectedObject%** e **%VirusName%** são usadas somente em mensagens de alerta de ameaça, enquanto **%ErrorDescription%** é usada somente em mensagens de evento.

Utilizar caracteres do alfabeto local - Converte uma mensagem de email para a codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").

Utilizar codificações de caracteres locais - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

4.6.1.13 Selecionar amostra para análise

A caixa de diálogo de envio de arquivo permite enviar um arquivo ou site para a ESET para fins de análise e pode ser acessada em **Ferramentas** > **Mais ferramentas** > **Enviar arquivo para análise**. Se você detectar um arquivo com comportamento suspeito no seu computador ou um site suspeito na internet, poderá enviá-lo para o Laboratório de pesquisa da ESET para análise. Se for detectado que o arquivo é um aplicativo ou site malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/ZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, o site do qual fez o download).

OBSERVAÇÃO: Antes de enviar um arquivo para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o arquivo não foi detectado
- o arquivo foi detectado incorretamente como uma ameaça

Você não receberá uma resposta, a não ser que mais informações sejam necessárias para a análise.

Selecione a descrição no menu suspenso **Motivo para envio do arquivo** mais adequada à sua mensagem:

- **Arquivo suspeito**
- **Site suspeito** (um site que está infectado por algum malware),
- **Arquivo falso positivo** (arquivo que é detectado como uma infecção, mas que não está infectado),
- **Site falso positivo**
- **Outros**

Arquivo/Site - O caminho do arquivo ou site que você pretende enviar.

Email de contato - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias, pois a cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios.

4.6.1.14 Microsoft Windows® update

O recurso de atualização do Windows é um componente importante de proteção de usuários contra software malicioso. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET Smart Security o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas para download.
- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. Assim, as informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

4.7 Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa.

Usando a ferramenta Gráficos, é possível ajustar a aparência visual do programa e os efeitos usados.

Ao configurar Alertas e notificações, você pode alterar o comportamento de alertas de ameaças detectadas e notificações do sistema. Esses recursos podem ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área Janelas de notificação ocultas. Aqui é possível verificar o status dessas notificações, mostrar mais detalhes ou removê-las dessa janela.

Para obter a máxima segurança do seu software, você pode evitar quaisquer alterações não autorizadas protegendo as configurações com uma senha com a ajuda da ferramenta Configuração de acesso.

O Menu de contexto é exibido após um clique com o botão direito do mouse em um objeto. Utilize essa ferramenta para integrar os elementos de controle do ESET Smart Security no menu de contexto.

4.7.1 Elementos da interface do usuário

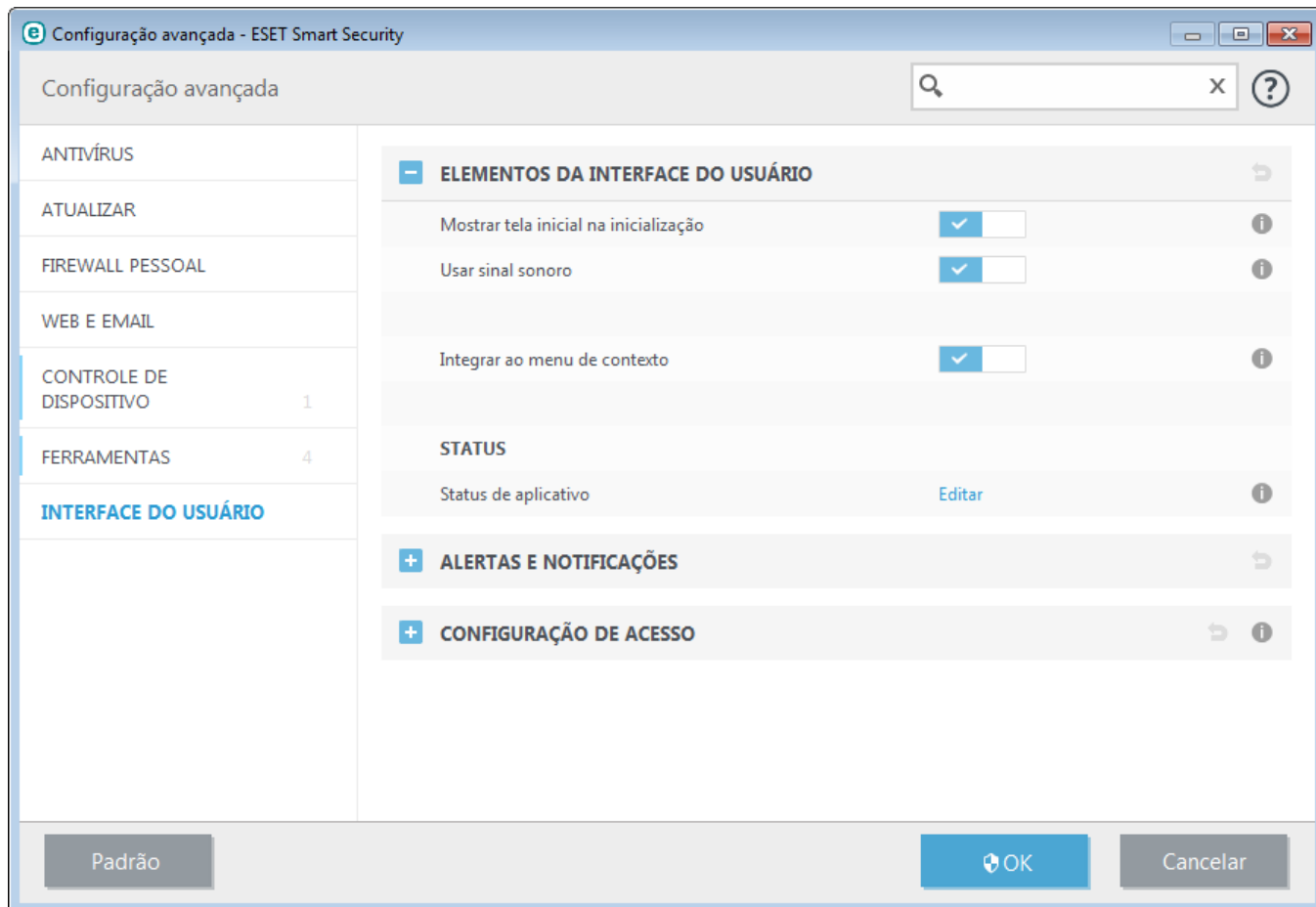
As opções de configuração da interface do usuário no ESET Smart Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** > **Elementos da interface do usuário** da árvore Configuração avançada do ESET Smart Security.

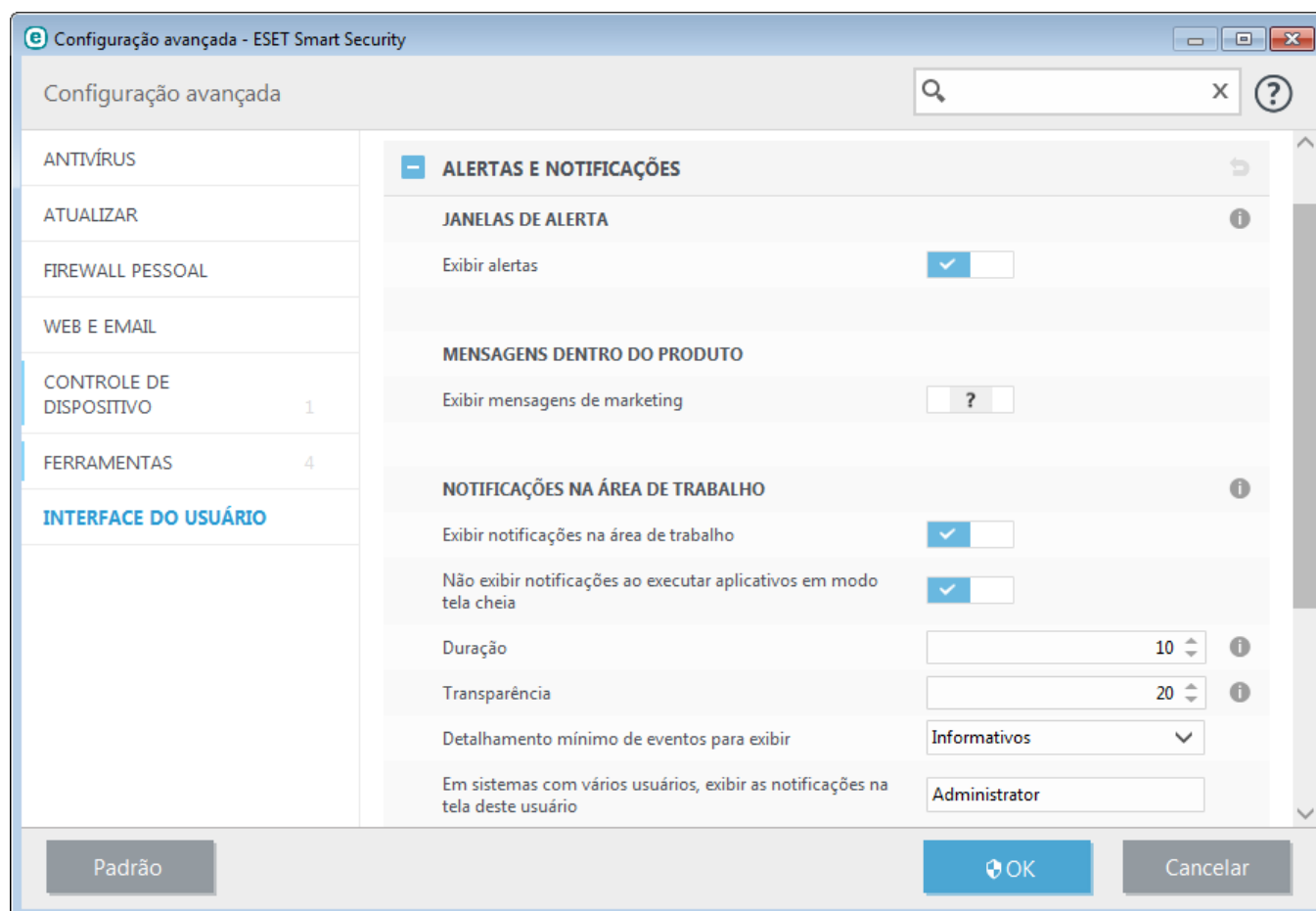
Se desejar desativar a tela inicial do ESET Smart Security, desmarque a opção **Mostrar tela inicial na inicialização**.

Se você quiser que o ESET Smart Security reproduza um som quando ocorrerem eventos importantes durante um rastreamento, por exemplo quando uma ameaça é descoberta ou quando a verificação for concluída, selecione **Usar sinal sonoro**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Smart Security no menu de contexto.

Status

Status de aplicativo - Clique no botão **Editar** para gerenciar (desativar) status que são exibidos no painel **Status da proteção** no menu principal.

4.7.2 Alertas e notificações

A seção **Alertas e notificações** em **Interface do usuário** permite que você configure como os alertas de ameaças e as notificações do sistema (por exemplo, mensagens de atualização bem-sucedida) são tratados no ESET Smart Security. Você também pode definir a hora e o nível de transparência das notificações da bandeja do sistema (aplica-se somente aos sistemas compatíveis com notificações na bandeja do sistema).

Janelas de alerta

Desativar a opção **Exibir alertas** cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Mensagens dentro do produto

Exibir mensagens de marketing - As mensagens dentro do produto foram feitas para informar os usuários ESET sobre novidades e outras comunicações. Desative esta opção se não quiser receber mensagens de marketing.

Notificações na área de trabalho

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar as notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**.

Ativar **Não exibir notificações ao executar aplicativos em modo tela cheia** para suprimir todas as notificações não interativas. Opções mais detalhadas, como o tempo de exibição e a transparência da janela de notificação, podem ser modificadas a seguir.

O menu suspenso **Detalhamento mínimo de eventos para exibir** permite selecionar o nível de gravidade de alertas e notificações a serem exibidos. As opções disponíveis são:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus , firewall integrado, etc...).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

Caixas de mensagens

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

Mensagens de confirmação - Mostra a você uma lista de mensagens de confirmação que você pode selecionar para serem exibidas ou não.

4.7.2.1 Configuração avançada

No menu suspenso **Detalhamento mínimo de eventos para exibir**, é possível selecionar o nível de gravidade inicial dos alertas e das notificações a serem exibidos.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como *"Erro ao fazer download de arquivo"* e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, a firewall pessoal, etc...).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

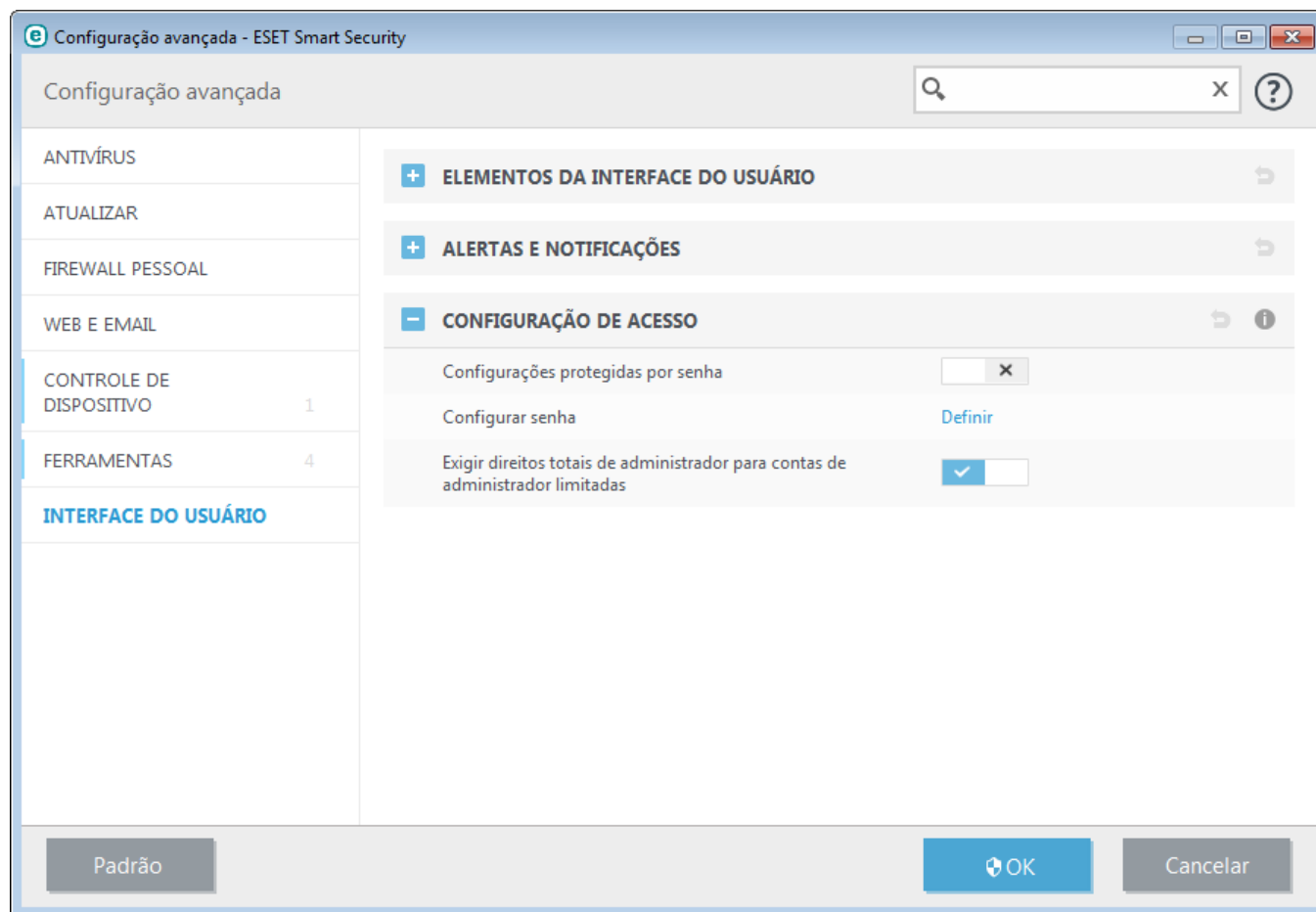
4.7.3 Janelas de notificação ocultas

Se a opção **Não exibir esta mensagem novamente** foi selecionada para qualquer janela de notificação (alerta) que foi exibida anteriormente, ela aparecerá na lista de janelas de notificações ocultas. As ações que agora são executadas automaticamente serão exibidas na coluna **Confirmar**.

Mostrar - Mostra uma visualização das janelas de notificação que não são exibidas no momento e para as quais uma ação automática está configurada.

Remover - Remove itens da lista de **Caixas de mensagens ocultas**. Todas as janelas de notificação removidas da lista serão exibidas novamente.

4.7.4 Configuração do acesso

As configurações do ESET Smart Security são uma parte essencial de sua política de segurança. Modificações não autorizadas podem colocar em risco a estabilidade e a proteção do seu sistema. Para evitar modificações não autorizadas, os parâmetros de configuração do ESET Smart Security podem ser protegidos por senha.

Configurações protegidas por senha - Indica as configurações com senha. Clique para abrir a janela Configuração de senha.

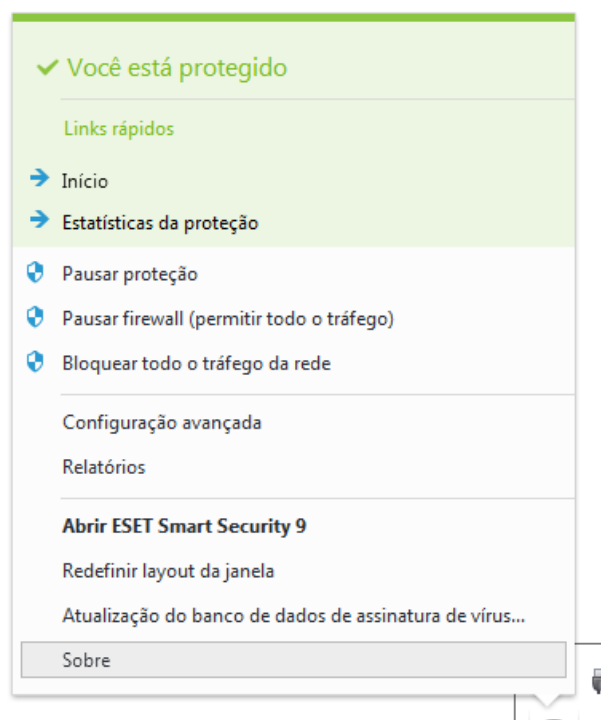
Para definir uma senha para proteger os parâmetros de configuração, clique em **Definir**.

Exigir direitos totais de administrador para contas de administrador limitadas - Selecione para solicitar que o usuário atual (se ele não tiver direitos de administrador) digite o nome de usuário e a senha de administrador quando modificar determinados parâmetros do sistema (semelhante ao UAC no Windows Vista e Windows 7). Essas modificações incluem a desativação dos módulos de proteção ou a desativação do firewall. Em sistemas Windows XP nos quais o UAC não estiver em execução, os usuários terão a opção **Exigir direitos de administrador (sistema sem suporte UAC)** disponível.

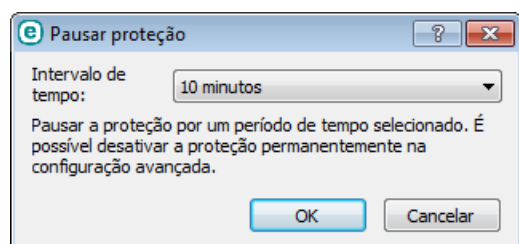
Apenas vara Windows XP:

Exigir direitos de administrador (sistema sem suporte UAC) - Ative esta opção para que o ESET Smart Security peça as credenciais do administrador.

4.7.5 Menu do programa

Estão disponíveis alguns dos recursos e opções de configuração mais importantes clicando com o botão direito do mouse no ícone da bandeja do sistema .

Links rápidos - Exibe as partes mais usadas do ESET Smart Security. Você pode acessar rapidamente esses objetos a partir do menu do programa.

Pausar proteção - Exibe a caixa de diálogo de confirmação que desativa a Proteção antivírus e antispyware, que protege contra ataques de sistema malicioso controlando arquivos e a comunicação via web e por emails.

O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção antivírus e antispyware será desativada.

Pausar firewall (permitir todo o tráfego) - Alterna o firewall para o estado inativo. Para obter mais informações, consulte Rede.

Bloquear todo o tráfego da rede - Bloqueia todo o tráfego da rede. É possível reativar clicando em **Parar de bloquear todo o tráfego de rede**.

Configuração avançada - Selecione essa opção para acessar a árvore **Configuração avançada**. Existem também outras formas de abrir as Configurações avançadas, como, por exemplo, pressionando a tecla F5 ou navegando até **Configuração** > **Configuração avançada**.

Arquivos de log - Os arquivos de log contêm informações sobre eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas.

Ocultar ESET Smart Security - Oculta a janela do ESET Smart Security da tela.

Redefinir layout da janela - Redefine a janela do ESET Smart Security para seu tamanho e posição padrão na tela.

Ative seu produto... - Selecione esta opção se ainda não tiver ativado seu produto de segurança da ESET, ou reinsira

as credenciais de ativação do produto depois de renovar sua licença.

Atualização do banco de dados de assinatura de vírus - Inicia a atualização do banco de dados de assinatura de vírus para garantir seu nível de proteção em relação ao código malicioso.

Sobre - As informações do sistema fornecem detalhes sobre a versão instalada do ESET Smart Security e os componentes do programa instalados. Aqui, você também pode encontrar a data de expiração de licença e informações sobre o sistema operacional e os recursos do sistema.

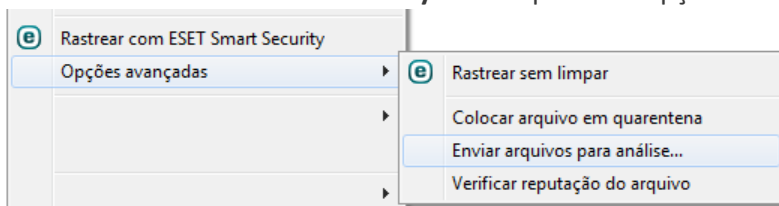
4.7.6 Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse em um objeto. O menu relaciona todas as ações que você pode realizar em um objeto.

É possível integrar os elementos de controle do ESET Smart Security no menu de contexto. Opções de configuração mais detalhadas para essa funcionalidade estão disponíveis na árvore Configuração avançada em **Interface do usuário** > **Menu de contexto**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Smart Security no menu de contexto.

As seguintes opções estão disponíveis no menu suspenso **Tipo de menu**:

- **Completo (rastrear primeiro)** - Ativa todas as opções do menu de contexto, o menu principal exibirá a opção **Rastrear sem limpar com o ESET Smart Security** como a primeira opção e **Rastrear e limpar** como o item no segundo nível.
- **Completo (limpar primeiro)** - Ativa todas as opções do menu de contexto, o menu principal exibirá a opção **Rastrear com ESET Smart Security** como a primeira opção e **Rastrear sem limpar** como o item no segundo nível.

- **Apenas rastrear** - Apenas **Rastrear sem limpar o ESET Smart Security** será exibido no menu de contexto.
- **Apenas limpar** - Apenas **Rastrear com o ESET Smart Security** será exibido no menu de contexto.

5. Usuário avançado

5.1 Gerenciador de perfil

O gerenciador de perfil é usado em duas seções no ESET Smart Security - **Rastreamento sob demanda do computador** e **Atualizar**.

Rastrear o computador

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Antivírus** > **Rastreamento sob demanda do computador** > **Básico** > **Lista de perfis**. A janela **Gerenciador de perfil** inclui o menu suspenso **Perfil selecionado** que lista perfis de rastreamento existentes e a opção de criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de **Rastrear seu computador** seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

Atualizar

O editor de perfil na seção de configuração da Atualização permite que os usuários criem novos perfis de atualização. Crie e use os seus próprios perfis personalizados (isto é, outros que não sejam o padrão **Meu perfil**) somente se o seu computador usar diversos modos de conexão com os servidores de atualização.

Por exemplo, um laptop que normalmente se conecta ao servidor local (Mirror) na rede local, mas faz os downloads das atualizações diretamente dos servidores de atualização da ESET quando está desconectado da rede local (em viagem de negócios, por exemplo) pode usar dois perfis: o primeiro para conectar ao servidor local; o segundo para conectar aos servidores da ESET. Quando esses perfis estiverem configurados, navegue até **Ferramentas** > **Agenda** e edite os parâmetros da tarefa de atualização. Designe um perfil como primário e outro como secundário.

Perfil selecionado - O perfil de atualização atualmente usado. Para mudar, escolha um perfil no menu suspenso.

Adicionar... - Criar novos perfis de atualização.

A parte inferior da janela lista os perfis existentes.

5.2 Atalhos do teclado

Para uma melhor navegação no seu produto ESET, os seguintes atalhos de teclado podem ser utilizados:

F1	abre as páginas da Ajuda
F5	abre a Configuração avançada
Up/Down	permite a navegação no produto por itens
-	recolhe os nós da árvore de Configuração avançada
TAB	move o cursor em uma janela
Esc	fecha a janela da caixa de diálogo ativa

5.3 Diagnóstico

O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, *ekrn*). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir os problemas do ESET Smart Security. Clique no menu suspenso ao lado de **Tipo de despejo** e selecione uma das três opções disponíveis:

- Selecione **Desativar** (padrão) para desativar esse recurso.
- **Mini** - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Este tipo de arquivo de despejo pode ser útil quando o espaço é limitado, no entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- **Completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo para inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.

Ativar registro em relatório avançado do Firewall pessoal - Registrar todos os dados de rede que passam pelo Firewall pessoal no formato PCAP para ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados ao Firewall pessoal.

Ativar registro em relatório avançado de Filtragem de protocolo - Registrar todos os dados passando pelo mecanismo de Filtragem de protocolo em formato PCAP para ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados a Filtragem de protocolo.

Os arquivos de relatório podem ser encontrados em:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics no Windows Vista e versões posteriores ou *C:\Documentos e configurações\Todos os usuários\...* em versões anteriores do Windows.

Diretório de destino – Diretório no qual o despejo durante a falha será gerado.

Abrir pasta de diagnóstico - Clique em **Abrir** para abrir esse diretório em uma nova janela do *Windows explorer*.

5.4 Importar e exportar configurações

Você pode importar ou exportar seu arquivo de configuração .xml personalizado do ESET Smart Security do menu **Configuração**.

A importação e a exportação dos arquivos de configuração serão úteis caso precise fazer backup da configuração atual do ESET Smart Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais em diversos sistemas. Os usuários podem importar facilmente um arquivo *.xml* para transferir essas configurações.

A importação de uma configuração é muito fácil. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações** e selecione **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão **...** para procurar o arquivo de configuração que deseja importar.

As etapas para exportar uma configuração são muito semelhantes. Na janela principal do programa, clique em **Configuração** > **Importar e exportar configurações**. Selecione a opção **Exportar configurações** e insira o nome de arquivo do arquivo de configuração (ou seja, *export.xml*). Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

OBSERVAÇÃO: Você pode encontrar um erro ao exportar configurações se não tiver direitos suficientes para gravar o arquivo exportado no diretório especificado.

5.5 Detecção em estado ocioso

As configurações da detecção em estado ocioso podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Detecção em estado ocioso**. Essas configurações especificam um acionador para Rastreamento em estado ocioso, quando:

- a proteção de tela estiver em execução,
- o computador estiver bloqueado,
- um usuário efetuar logoff.

Use as caixas de seleção de cada estado para ativar ou desativar os diferentes acionadores de detecção de estado ocioso.

5.6 ESET SysInspector

5.6.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada em soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões são idênticas em função e têm os mesmos controles de programa. A única diferença é como os resultados são gerenciados. As versões integrada e separada permitem exportar snapshots do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os snapshots do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator). Para obter mais informações, consulte a seção ESET SysInspector como parte do ESET Smart Security.

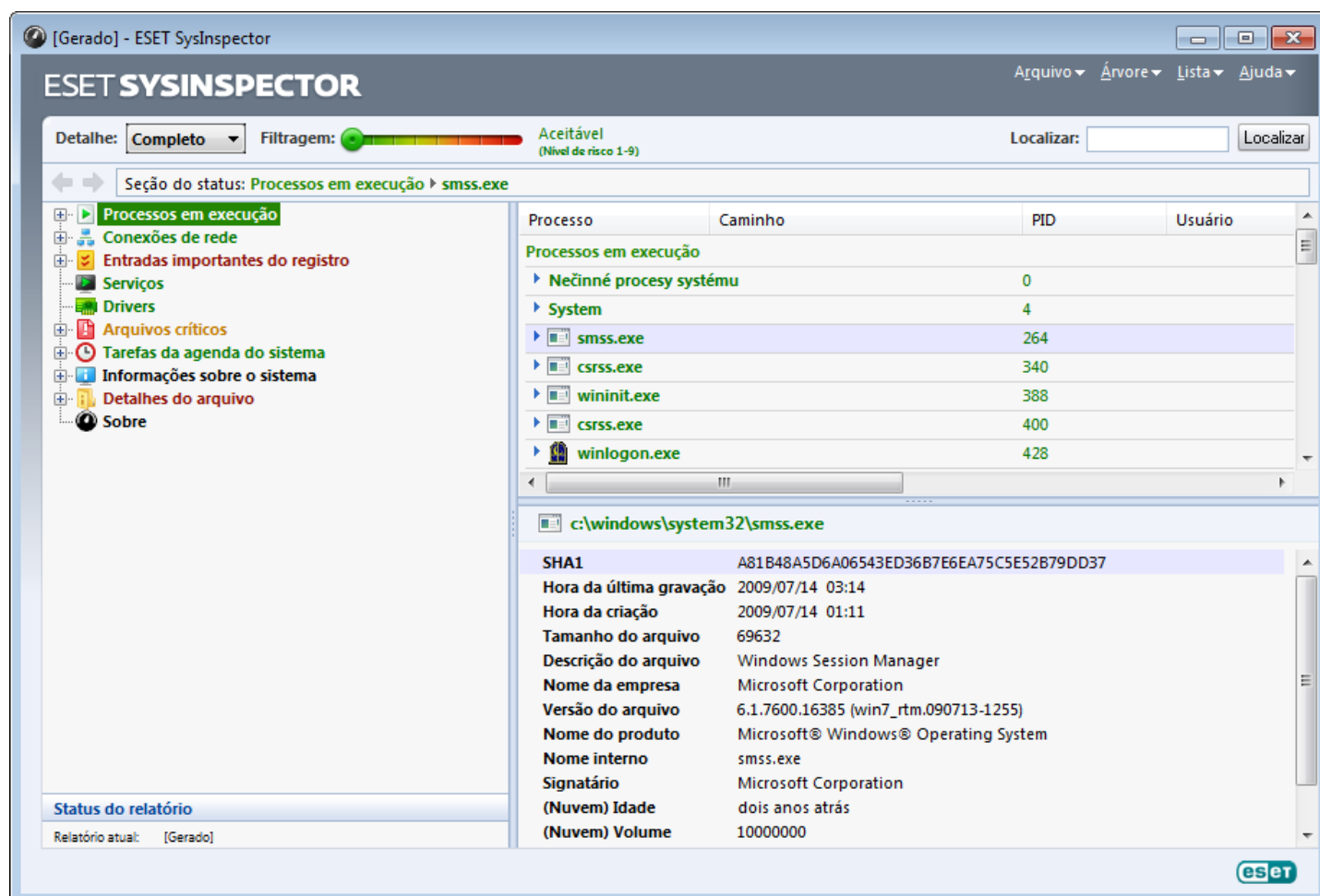
Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

5.6.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo *SysInspector.exe* obtido por download no site da ESET. Se já tiver uma das soluções ESET Security instalada, é possível executar o ESET SysInspector diretamente a partir do menu Iniciar (clique em **Programas** > **ESET** > **ESET Smart Security**).

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos.

5.6.2 Interface do usuário e uso do aplicativo

Para maior clareza, a janela do programa principal é dividida em quatro seções principais - Controles do programa localizados na parte superior da janela do programa principal, a janela Navegação à esquerda, a janela Descrição à direita e a janela Detalhes, na parte inferior da janela do programa principal. A seção Status do relatório lista os parâmetros básicos de um relatório (filtro usado, tipo do filtro, se o relatório é resultado de uma comparação, etc.).

5.6.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um relatório armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um relatório **Adequado para envio**. Neste formulário, o relatório omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente arrastando e soltando-os na janela do programa principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela do programa principal para facilitar o trabalho com as informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe menos detalhes usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para solucionar problemas muito específicos.

Filtragem

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver totalmente à esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante totalmente à direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens identificados como de risco 6 a 9 podem colocar a segurança em risco. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrou esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Comparar

Ao comparar dois relatórios, você pode optar por exibir todos os itens, exibir apenas os itens adicionados, exibir apenas os itens removidos ou exibir apenas os itens substituídos.

Localizar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, verifique se os arquivos são realmente perigosos ou desnecessários.

5.6.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do relatório. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo e o nível de risco do arquivo.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados constantemente e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como Serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de tarefas do Windows em um intervalo/horário especificado.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas e direitos do usuário.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista de módulos do programa.

5.6.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	abre o relatório existente
Ctrl+S	salva os relatórios criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	aceitável, nível de risco 1-9, os itens são exibidos
2	aceitável, nível de risco 2-9, os itens são exibidos
3	aceitável, nível de risco 3-9, os itens são exibidos
4, U	desconhecido, nível de risco 4-9, os itens são exibidos
5	desconhecido, nível de risco 5-9, os itens são exibidos
6	desconhecido, nível de risco 6-9, os itens são exibidos
7, B	perigoso, nível de risco 7-9, os itens são exibidos
8	perigoso, nível de risco 8-9, os itens são exibidos
9	perigoso, nível de risco 9, os itens são exibidos
-	diminui o nível de risco
+	aumenta o nível de risco
Ctrl+9	modo de filtragem, nível igual ou superior
Ctrl+0	modo de filtragem, somente nível igual

Exibir

Ctrl+5	exibição por fornecedor, todos os fornecedores
Ctrl+6	exibição por fornecedor, somente Microsoft
Ctrl+7	exibição por fornecedor, todos os outros fornecedores
Ctrl+3	exibe detalhes completos
Ctrl+2	exibe detalhes da mídia
Ctrl+1	exibição básica
Backspace	move um passo para trás
Espaço	move um passo para a frente
Ctrl+W	expande a árvore
Ctrl+Q	recolhe a árvore

Outros controles

Ctrl+T	vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	exibe informações básicas sobre um item
Ctrl+A	exibe informações completas sobre um item

Ctrl+C	copia a árvore do item atual
Ctrl+X	copia itens
Ctrl+B	localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	abre a entrada correspondente no editor do registro
Ctrl+Z	copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	alterna para o campo de pesquisa
Ctrl+D	fecha os resultados da pesquisa
Ctrl+E	executa script de serviços

Comparação

Ctrl+Alt+O	abre o relatório original/comparativo
Ctrl+Alt+R	cancela a comparação
Ctrl+Alt+1	exibe todos os itens
Ctrl+Alt+2	exibe apenas os itens adicionados; o relatório mostrará os itens presentes no relatório atual
Ctrl+Alt+3	exibe apenas os itens removidos; o relatório mostrará os itens presentes no relatório anterior
Ctrl+Alt+4	exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	exibe apenas as diferenças entre os relatórios
Ctrl+Alt+C	exibe a comparação
Ctrl+Alt+N	exibe o relatório atual
Ctrl+Alt+P	exibe o relatório anterior

Diversos

F1	exibe a ajuda
Alt+F4	fecha o programa
Alt+Shift+F4	fecha o programa sem perguntar
Ctrl+I	estatísticas de relatórios

5.6.2.3 Comparar

O recurso Comparar permite que o usuário compare dois relatórios existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os relatórios. Ele é adequado se você desejar manter controle das alterações no sistema, uma ferramenta útil para detectar código malicioso.

Após ser iniciado, o aplicativo criará um novo relatório que será exibido em uma nova janela. Clique em **Arquivo** > **Salvar relatório** para salvar um relatório em um arquivo. Os relatórios podem ser abertos e visualizados posteriormente. Para abrir um relatório existente, clique em **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um relatório de cada vez.

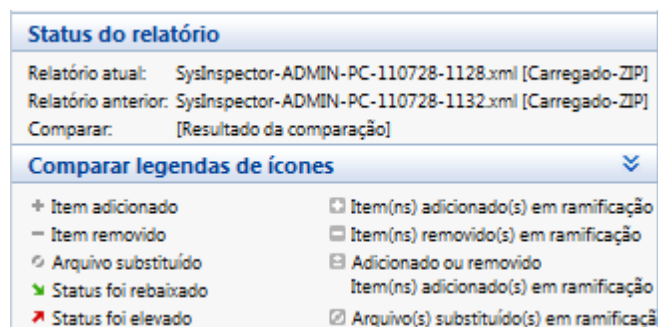
O benefício de comparar dois relatórios é que você pode visualizar um relatório ativo no momento e um relatório salvo em um arquivo. Para comparar relatórios, clique em **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O relatório selecionado será comparado com o relatório ativo na janela principal do programa. O relatório comparativo exibirá apenas as diferenças entre esses dois relatórios.

OBSERVAÇÃO: Caso compare dois relatórios, clique em **Arquivo** > **Salvar relatório** para salvá-lo como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir este arquivo posteriormente, os relatórios contidos serão comparados automaticamente.

Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os relatórios comparados.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- novo valor, não presente no relatório anterior
- a seção de estrutura em árvore contém novos valores
- valor removido, presente apenas no relatório anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no relatório anterior
- o nível de risco aumentou / era menor no relatório anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos relatórios que estão sendo comparados.

Qualquer relatório comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois relatórios, clique em **Arquivo** > **Comparar relatórios**. O programa criará um relatório comparativo mostrando as diferenças entre os relatórios.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

5.6.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar relatório diretamente a partir da linha de comando sem operar a GUI
/privacy	gerar relatório com informações confidenciais omitidas
/zip	salvar o relatório de resultado no arquivo zip compactado
/silent	suprimir a janela de progresso ao gerar o relatório da linha de comando
/blank	iniciar o ESET SysInspector sem gerar/carregar o relatório

Exemplos

Uso:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Para carregar relatório específico diretamente no navegador, use: *SysInspector.exe .\clientlog.xml*
Para gerar relatório a partir da linha de comando, use: *SysInspector.exe /gen=.\mynewlog.xml*
Para gerar relatório excluindo informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dois relatórios e procurar diferenças, use: *SysInspector.exe new.xml old.xml*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

5.6.4 Script de serviços

O script de serviços é uma ferramenta que oferece ajuda a clientes que usam o ESET SysInspector, removendo facilmente objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o relatório modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As alterações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador está infectado por um vírus que não é detectado pelo seu programa antivírus, siga estas instruções passo a passo:

1. Execute o ESET SysInspector para gerar um novo snapshot do sistema.
2. Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Shift e selecione o último item para marcar todos os itens.
3. Clique com o botão direito do mouse nos objetos selecionados e selecione **Exportar as seções selecionadas para script de serviços**.
4. Os objetos selecionados serão exportados para um novo relatório.
5. Esta é a etapa mais crucial de todo o procedimento: abra o novo relatório e altere o atributo – para + para todos os objetos que desejar remover. Certifique-se de não marcar nenhum arquivo/objeto importante do sistema operacional.
6. Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o seu script.
7. Clique em **OK** para executar o script.

5.6.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione **Exportar todas as seções para script de serviços** ou **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois relatórios estiverem sendo comparados.

5.6.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, há informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do relatório (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando você executar o script, os drivers selecionados serão interrompidos. Observe que alguns drivers não permitirão eles mesmos a interrupção.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos que são críticos para o funcionamento correto do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos, ou serão restaurados seus valores padrão originais.

10) Tarefas agendadas

Esta seção contém informações sobre os as tarefas agendadas.

Exemplo:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma caixa de diálogo confirmará que o script foi executado com sucesso.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

5.6.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um relatório?

O ESET SysInspector pode criar um relatório da configuração do computador. Para salvar um relatório, clique em **Arquivo** > **Salvar relatório** na janela do programa principal. Os relatórios são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*, com uma convenção de nomenclatura de arquivos de "SysInpsector-%NOMECOMPUTADOR%-AAMMDD-HHMM.XML". Você pode alterar o local e o nome do relatório para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o relatório do ESET SysInspector?

Para visualizar um relatório criado pelo ESET SysInspector, execute o programa e clique em **Arquivo** > **Abrir relatório** na janela do programa principal. Você também pode arrastar e soltar relatórios no aplicativo ESET SysInspector. Se você precisar visualizar os relatórios do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os relatórios para visualização. Por motivo de segurança, os Windows Vista/7 podem não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do relatório? E um SDK?

Atualmente, não há uma especificação para o relatório nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro deles.

Um nível de risco "6 – Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles também podem examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporta como um rootkit, o usuário será exposto ao risco de danos ou roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validando usando essas informações. Se uma assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Se o arquivo CAT pertinente for encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Arquivos de Programas\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

5.6.6 ESET SysInspector como parte do ESET Smart Security

Para abrir a seção do ESET SysInspector no ESET Smart Security, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com snapshots: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar... ou excluir snapshots, utilize os botões correspondentes localizados abaixo da lista de snapshots na janela do ESET SysInspector. Essas opções também estão disponíveis no menu de contexto. Para exibir o instantâneo do sistema selecionado, selecione **Mostrar** no menu de contexto. Para exportar o snapshot selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**.

Abaixo, há uma descrição detalhada das opções disponíveis:

- **Comparar** – permite comparar dois relatórios existentes. Ela é adequada se você desejar controlar alterações entre o relatório atual e um relatório anterior. Para que essa opção entre em vigor, é necessário selecionar dois snapshots a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para localizar o progresso de criação do snapshot (do snapshot gerado no momento), veja a coluna **Status**. Todos os snapshots concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** - Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

5.7 Linha de comando

O módulo antivírus do ESET Smart Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat"). Uso para o rastreamento por linha de comando da ESET:

```
ecls [OPTIONS..] FILES..
```

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções

/base-dir=PASTA	carregar módulos da PASTA
/quar-dir=PASTA	PASTA de quarentena
/exclude=MÁSCARA	excluir arquivos que correspondem à MÁSCARA do rastreamento

/subdir	rastrear subpastas (padrão)
/no-subdir	não rastrear subpastas
/max-subdir-level=NÍVEL	subnível máximo de pastas dentro de pastas para rastrear
/symlink	seguir links simbólicos (padrão)
/no-symlink	ignorar links simbólicos
/ads	rastrear ADS (padrão)
/no-ads	não rastrear ADS
/log-file=ARQUIVO	registrar o relatório em ARQUIVO
/log-rewrite	substituir arquivo de saída (padrão - acrescentar)
/log-console	registrar saída para console (padrão)
/no-log-console	não registrar saída para console
/log-all	também registrar arquivos limpos
/no-log-all	não registrar arquivos limpos (padrão)
/aind	mostrar indicador de atividade
/auto	rastrear e limpar automaticamente todos os discos locais

Opções do scanner

/files	rastrear arquivos (padrão)
/no-files	não rastrear arquivos
/memory	rastrear memória
/boots	rastrear setores de inicialização
/no-boots	não rastrear setores de inicialização (padrão)
/arch	rastrear arquivos compactados (padrão)
/no-arch	não rastrear arquivos compactados
/max-obj-size=TAMANHO	rastrear apenas arquivos com menos de TAMANHO megabytes (padrão 0 = sem limite)
/max-arch-level=NÍVEL	subnível máximo de arquivos dentro de arquivos (arquivos aninhados) para rastrear
/scan-timeout=LIMITE	rastrear arquivos pelo LIMITE máximo de segundos
/max-arch-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado se eles tiverem menos de TAMANHO (padrão 0 = sem limite)
/max-sfx-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado de auto-extração se eles tiverem menos de TAMANHO megabytes (padrão 0 = sem limite)
/mail	rastrear arquivos de email (padrão)
/no-mail	não rastrear arquivos de email
/mailbox	rastrear caixas de correio (padrão)
/no-mailbox	não rastrear caixas de correio
/sfx	rastrear arquivos compactados de auto-extração (padrão)
/no-sfx	não rastrear arquivos compactados de auto-extração
/rtp	rastrear empacotadores em tempo real (padrão)
/no-rtp	não rastrear empacotadores em tempo real
/unsafe	rastrear por aplicativos potencialmente inseguros
/no-unsafe	não rastrear por aplicativos potencialmente inseguros (padrão)
/unwanted	rastrear por aplicativos potencialmente indesejados
/no-unwanted	não rastrear por aplicativos potencialmente indesejados (padrão)
/suspicious	rastrear aplicativos suspeitos (padrão)
/no-suspicious	não rastrear aplicativos suspeitos
/pattern	usar assinaturas (padrão)
/no-pattern	não usar assinaturas
/heur	ativar heurística (padrão)
/no-heur	desativar heurística
/adv-heur	ativar heurística avançada (padrão)
/no-adv-heur	desativar heurística avançada
/ext=EXTENSÕES	verificar somente EXTENSÕES delimitadas por dois pontos
/ext-exclude=EXTENSÕES	excluir do rastreamento EXTENSÕES delimitadas por dois pontos

/clean-mode=MODO	utilizar MODO de limpeza para objetos infectados

As opções disponíveis são:

- **none** (nenhuma) - não ocorrerá nenhuma limpeza automática.
- **standard** (padrão) - o ecls.exe tentará limpar ou excluir automaticamente os arquivos infectados.
- **strict** (rígida) - o ecls.exe tentará limpar ou excluir automaticamente todos os arquivos infectados sem intervenção do usuário (você não será avisado antes de os arquivos serem excluídos).
- **rigorous** (rigorosa) - o ecls.exe excluirá arquivos sem tentar limpá-los, independentemente de quais arquivos sejam.
- **delete** (excluir) - o ecls.exe excluirá arquivos sem tentar limpá-los, mas não excluirá arquivos importantes, como arquivos do sistema Windows.

/quarantine	copiar arquivos infectados para Quarentena (completa a ação realizada enquanto ocorre a limpeza)
/no-quarantine	não copiar arquivos infectados para Quarentena

Opções gerais

/help	mostrar ajuda e sair
/version	mostrar informações de versão e sair
/preserve-time	manter último registro de acesso

Códigos de saída

0	nenhuma ameaça encontrada
1	ameaça encontrada e removida
10	alguns arquivos não puderam ser rastreados (podem conter ameaças)
50	ameaça encontrada
100	erro

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

6. Glossário

6.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

6.1.1 Vírus

Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro. Quanto ao termo "vírus", ele é frequentemente usado de maneira incorreta para significar qualquer tipo de ameaça. Essa utilização está gradualmente sendo superada e substituída por um termo mais preciso "malware" (software malicioso).

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o código malicioso é chamado e executado antes da execução do aplicativo original. Um vírus pode infectar qualquer arquivo que tenha permissão de gravação dada pelo usuário.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

Se o computador estiver infectado com um vírus e a limpeza não for possível, envie-o para o Laboratório de pesquisa da ESET para análise. Em certos casos os arquivos infectados podem ser modificados a ponto de uma limpeza não ser possível e os arquivos precisarem ser substituídos por uma cópia limpa.

6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se propagar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms propagam-se para os endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de horas ou mesmo minutos após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

6.1.3 Cavalos de Troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de ameaças que tentam se apresentar como programas úteis, enganando assim os usuários para executá-los.

Dado que Cavalos de Troia são uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** - Programas maliciosos com a capacidade de fazer o download de outras ameaças da Internet.
- **Dropper** - Programas maliciosos com a capacidade para instalar outros tipos de malware em computadores comprometidos.
- **Backdoor** - Programas maliciosos que se comunicam com atacantes remotos, permitindo que eles acessem o computador e assumam o seu controle.
- **Keylogger** - (keystroke logger) - Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- **Dialer** - Programas maliciosos projetados para se conectar aos números premium-rate em vez do provedor de serviços de Internet do usuário. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.

Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele contém códigos maliciosos.

6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1. Quando eles tentam acessar um sistema: Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2. Quando eles estão ocultos para os testes usuais: os usuários do ESET Smart Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

6.1.5 Adware

Adware é abreviação de “advertising-supported software” (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage deste. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

6.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

6.1.7 Empacotadores

O empacotador é um executável de extração automática do tempo de execução que realiza vários tipos de malware em um único pacote.

Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Os empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando mais difícil a detecção e remoção do malware.

6.1.8 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Smart Security fornece a opção de detectar tais ameaças.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

6.1.9 Aplicativos potencialmente indesejados

Um aplicativo potencialmente indesejado é um programa que contém adware, instala barras de ferramentas ou tem outros objetivos pouco claros. Existem algumas situações em um usuário pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

Aviso - Ameaça em potencial encontrada

Quando um aplicativo potencialmente indesejado é detectado, você poderá decidir qual ação realizar:

1. **Limpar/Desconectar**: Esta opção encerra a ação e evita que uma possível ameaça entre no sistema.
2. **Ignorar**: Essa opção permite que a ameaça em potencial entre em seu sistema.
3. Para permitir que o aplicativo seja executado no seu computador no futuro sem interrupções, clique em **Opções avançadas** e selecione a caixa de seleção ao lado de **Excluir da detecção**.

Quando um aplicativo potencialmente indesejado é detectado e não é possível limpar, uma janela de notificação **O endereço foi bloqueado** será exibida no canto inferior direito da tela. Para mais informações sobre este evento vá para **Ferramentas** > **Mais ferramentas** > **Relatórios** > **Sites filtrados** no menu principal.

Aplicativos potencialmente indesejados - Configurações

Ao instalar seu produto ESET, é possível decidir se vai ativar a detecção de aplicativos potencialmente não desejados, conforme exibido abaixo:

Aplicativos potencialmente indesejados podem instalar adware, barras de ferramentas ou ter outros recursos de programa indesejados e inseguros.

Essas configurações podem ser modificadas nas suas configurações de programa a qualquer momento. Para ativar ou desativar a detecção de Aplicativos potencialmente indesejados, inseguros ou suspeitos, siga essas instruções:

1. Abra seu produto ESET. Como abrir meu produto ESET?
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Antivírus** e ative ou desative as opções **Ativar detecção de aplicativos potencialmente não desejados**, **Ativar detecção de aplicativos potencialmente inseguros** e **Ativar detecção de Ativar detecção de aplicativos suspeitos** de acordo com suas preferências. Confirme clicando em **OK**.

Aplicativos potencialmente indesejados - Wrapper de software

Um wrapper de software é um tipo especial de modificação de aplicativo que é usado por alguns sites de hospedagem de arquivos. É uma ferramenta de terceiros que instala o programa que você planejou baixar, mas adiciona outros software, como barras de ferramentas ou adware. O software adicional também pode fazer alterações na página inicial do seu navegador ou nas configurações de pesquisa. Além disso, sites de hospedagem de arquivos muitas vezes não notificam o fabricante do software ou receptor do download que modificações foram feitas e não permite que seja possível optar por não obter uma modificação com facilidade. Por esses motivos, a ESET classifica wrapper de software como um tipo de aplicativo potencialmente indesejado para permitir aos usuários aceitarem ou não seu download.

Consulte o seguinte artigo da Base de Conhecimento ESET para obter uma versão atualizada desta página de ajuda.

6.1.10 Botnet

Um bot, ou um robô da web, é um programa de malware automatizado que rastreia blocos de endereços de rede e infecta computadores vulneráveis. Isso permite que hackers tomem o controle de vários computadores ao mesmo tempo e transformem esses computadores em bots (também conhecido como um zumbi). Normalmente os hackers usam bots para infectar um grande número de computadores, que formam uma rede ou um botnet. Quando um botnet está no seu computador, ele pode ser usado em ataques distribuídos de negação de serviço (DDoS), proxy e também podem ser usados para realizar tarefas automáticas na Internet sem o seu conhecimento (por exemplo: enviar spam, vírus ou roubar informações pessoais e particulares, como credenciais bancárias ou números de cartão de crédito).

6.2 Tipos de ataques remotos

Há muitas técnicas especiais que permitem que os agressores comprometam os sistemas remotos. Elas são divididas em diversas categorias.

6.2.1 Ataques DoS

DoS, ou *Denial of Service* (negação de serviço), é a tentativa de impedir que o computador ou a rede sejam acessados por seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reinicializados para que voltem a funcionar adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

6.2.2 Envenenamento de DNS

Através do envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são armazenadas em cache por um determinado período de tempo, permitindo que os agressores reescrevam as respostas do DNS dos endereços IP. Como resultado, os usuários que tentarem acessar os websites da Internet farão o download de vírus ou worms no lugar do seu conteúdo original.

6.2.3 Ataques de worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. Os worms da rede exploram as vulnerabilidades de segurança dos diversos aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação.

A maioria dos ataques dos worms (Sasser, SqlSlammer) podem ser evitados usando-se as configurações de segurança padrão do firewall, ou bloqueando as portas não usadas e desprotegidas. Também é fundamental manter o sistema operacional atualizado com os patches de segurança mais recentes.

6.2.4 Rastreamento de portas

O rastreamento de portas é usado para determinar se há portas abertas no computador em um host de rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e saída - ação crucial do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Tal uso é legítimo.

O rastreamento de porta é frequentemente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

6.2.5 Dessincronização TCP

A dessincronização TCP é uma técnica usada nos ataques do TCP Hijacking. Ela é acionada por um processo no qual o número sequencial dos pacotes recebidos difere do número sequencial esperado. Os pacotes com um número sequencial inesperado são dispensados (ou salvos no armazenamento do buffer, se estiverem presentes na janela de comunicação atual).

Na dessincronização, os dois pontos finais da comunicação dispensam os pacotes recebidos; esse é o ponto onde os agressores remotos são capazes de se infiltrar e fornecer pacotes com um número sequencial correto. Os agressores podem até manipular ou modificar a comunicação.

Os ataques TCP Hijacking têm por objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados usando autenticação para cada segmento TCP. Também é aconselhável usar as configurações recomendadas para os seus dispositivos de rede.

6.2.6 Relé SMB

O Relé SMB e o Relé SMB 2 são programas especiais capazes de executar um ataque contra computadores remotos. Os programas se aproveitam do protocolo de compartilhamento do arquivo Server Message Block que é embutido no NetBios. Se um usuário compartilhar qualquer pasta ou diretório dentro da LAN, provavelmente ele utilizará esse protocolo de compartilhamento de arquivo.

Dentro da comunicação de rede local, as criptografias da senha são alteradas.

O Relé SMB recebe uma conexão nas portas UDP 139 e 445, detecta os pacotes trocados pelo cliente e o servidor e os modifica. Após conectar e autenticar, o cliente é desconectado. O Relé SMB cria um novo endereço IP virtual. O novo endereço pode ser acessado usando o comando "net use \\192.168.1.1". O endereço pode então ser usado por qualquer uma das funções de rede do Windows. O Relé SMB detecta a comunicação do protocolo SMB, exceto para negociação e autenticação. Os agressores remotos podem usar o endereço IP enquanto o computador cliente estiver conectado.

O Relé SMB 2 funciona com o mesmo princípio do Relé SMB, exceto que ele usa os nomes do NetBios no lugar dos endereços IP. Os dois executam ataques "man-in-the-middle". Esses ataques permitem que os agressores remotos leiam, insiram e modifiquem as mensagens trocadas entre dois pontos finais de comunicação sem serem notados. Os computadores expostos a tais ataques frequentemente param de responder ou reiniciam inesperadamente.

Para evitar ataques, recomendamos que você use senhas ou chaves de autenticação.

6.2.7 Ataques ICMP

O ICMP (Protocolo de Controle de Mensagens da Internet) é um protocolo de Internet popular e amplamente utilizado. Ele é utilizado primeiramente por computadores em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar a fraqueza do protocolo ICMP. O protocolo ICMP é destinado para a comunicação unidirecional que não requer qualquer autenticação. Isso permite que os atacantes remotos disparem ataques chamados de DoS (negação de serviço) ou ataques que dão acesso a pessoas não autorizadas aos pacotes de entrada e de saída.

Exemplos típicos de um ataque ICMP são ping flood, flood de ICMP_ECHO e ataques de smurfs. Os computadores expostos ao ataque ICMP são significativamente mais lentos (isso se aplica a todos os aplicativos que utilizam a Internet) e têm problemas para conectarem-se à Internet.

6.3 Tecnologia ESET

6.3.1 Bloqueio de Exploit

O Bloqueio de exploit é feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Ele funciona monitorando o comportamento de processos em busca de atividades suspeitas que possam indicar um exploit.

Quando o Bloqueio de Exploit identifica um processo suspeito, ele pode interromper o processo imediatamente e registrar os dados sobre a ameaça, que são enviados ao sistema de nuvem do ThreatSense. Estes dados poderão ser processados pelo Laboratório de pesquisa da ESET e usados para proteger melhor todos os usuários contra ameaças desconhecidas e ataques novos (de malware recém-lançado para o qual não há solução pré-configurada).

6.3.2 Rastreamento de memória avançado

O Rastreamento de memória avançado funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação e/ou criptografia. Em casos onde a emulação comum ou heurística podem não detectar uma ameaça, o Rastreamento de memória avançado é capaz de identificar o comportamento suspeito e rastrear ameaças conforme elas se revelam na memória do sistema. Esta solução é eficaz contra malware que ainda esteja fortemente ofuscado.

Ao contrário do Bloqueio de exploit, O Rastreamento de memória avançado é um método de pós-execução, significando que existe um risco de alguma atividade maliciosa possa ter sido realizada antes de uma ameaça ser detectada, porém no caso de outras técnicas de detecção terem falhado ele oferece uma camada adicional de segurança.

6.3.3 Escudo de vulnerabilidade

O Escudo de vulnerabilidade é uma extensão para o Firewall pessoal que melhora a detecção de vulnerabilidades conhecidas no nível da rede. Ao implementar detecções para vulnerabilidades comuns em protocolos amplamente utilizados como o SMB, RPC e RDP, ele constrói uma outra camada de proteção importante contra a propagação de malware, ataques conduzidos pela rede e explorações de vulnerabilidades para os quais um ainda não foi lançado ou implantado um patch.

6.3.4 ThreatSense

Construído sobre o sistema de alerta precoce avançado do ThreatSense.Net®, o ESET LiveGrid® usa dados que os usuários ESET enviaram em todo o mundo e envia-os para o Laboratório de pesquisa ESET. Ao fornecer amostras suspeitas e metadados originais, o ESET LiveGrid® nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes. Pesquisadores de malware da ESET usam as informações para construir um instantâneo preciso sobre a natureza e abrangência das ameaças globais, que nos ajuda a concentrar nos alvos corretos. Os dados do ESET LiveGrid® desempenham um papel importante na definição de prioridades do nosso processamento automatizado.

Além disso, ele implementa um sistema de reputação que ajuda a melhorar a eficiência global de nossas soluções anti-malware. Quando um arquivo executável está sendo inspecionado no sistema de um usuário, seu hashtag é comparado pela primeiro contra um banco de dados de itens na lista de permissões e lista de proibições. Se ele for encontrado na lista de permissões, o arquivo inspecionado é considerado limpo e sinalizado para ser excluído de rastreamentos futuros. Se ele estiver na lista de proibições as ações apropriadas serão tomadas com base na natureza da ameaça. Se nenhuma correspondência for encontrada o arquivo é verificado completamente. Com base nos resultados deste rastreamento, os arquivos são classificados como ameaças ou não ameaças. Esta abordagem tem um impacto positivo significante no desempenho do rastreamento.

Este sistema de reputação permite uma detecção eficaz de amostras de malware, mesmo antes de suas assinaturas serem entregues para o computador do usuário através de um banco de dados de vírus atualizado (o que acontece várias vezes ao dia).

6.3.5 Proteção contra botnet

A proteção contra botnet descobre malware ao analisar seus protocolos de comunicação de rede. O botnet de malware é alterado frequentemente, em contraste com os protocolos de rede, que não foram alterados nos últimos anos. Essa nova tecnologia ajuda a ESET a combater qualquer malware que tente evitar ser detectado e tente conectar seu computador a uma rede botnet.

6.3.6 Bloqueio de Exploit do Java

O Bloqueio de Exploit do Java é uma extensão para a proteção de Bloqueio de Exploit. Ela monitora o Java e procura comportamentos semelhantes aos de exploit. Amostras bloqueadas podem ser encaminhadas para analisadores de malware, para que eles possam criar assinaturas para bloqueá-los em camadas diferentes (bloqueio de URL, download de arquivos, etc.).

6.3.7 Proteção de Atividade bancária e Pagamento

A Proteção de Atividade bancária e Pagamento representa uma camada de proteção adicional para transações on-line, pois seu navegador não protegido pode ser comprometido durante uma transação.

O ESET Smart Security contém uma lista embutida de sites pré-definidos que vão acionar a abertura de um navegador protegido. É possível adicionar um site ou editar a lista de sites na configuração do produto.

O uso de comunicação com criptografia HTTPS é necessário para realizar a navegação protegida. Para usar a navegação protegida, seu navegador da internet deve cumprir com os requisitos mínimos listados abaixo. Recomendamos fechar o navegador protegido depois de concluir as transações ou pagamentos on-line.

O número da versão do navegador exibido abaixo ou versão mais recente é necessário para usar o navegador protegido:

- Mozilla Firefox 24
- Internet Explorer 8
- Google Chrome 30

6.4 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. Flexível, rápido e direto, o email teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso - malware (códigos maliciosos). A inconveniência e o perigo para você são aumentados pelo fato de que os custos de envio são mínimos e os autores de spam têm muitas ferramentas para obter novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou à sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" - por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

6.4.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são o custo mínimo e um alto nível de objetividade. Além disso, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse tipo de publicidade é legítimo, desde que você tenha interesse em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o limite razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Geralmente, os autores dos emails não solicitados tentam mascarar o spam como mensagens legítimas.

6.4.2 Hoaxes

Um hoax é uma informação incorreta que é propagada pela Internet. Normalmente, os hoaxes são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

6.4.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por ex. instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

6.4.4 Reconhecimento de fraudes em spam

Geralmente, há alguns indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- O endereço do remetente não pertence a alguém da sua lista de contatos.
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma.
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais (números de contas bancárias, nomes de usuário e senhas, etc.)
- Está escrito em um idioma estrangeiro.
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo, "vaigra" em vez de "viagra", etc.

6.4.4.1 Regras

No contexto das soluções antispam e dos clientes de email, as regras são as ferramentas para manipular as funções do email. Elas são constituídas por duas partes lógicas:

1. Condição (por exemplo, uma mensagem recebida de um determinado endereço)
2. Ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada)

O número e a combinação de diversas regras com a solução antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

- 1. Condição: Uma mensagem de email recebida contém algumas palavras geralmente vistas nas mensagens de spam.
  2. Ação: Excluir a mensagem.

- 1. Condição: Uma mensagem de email recebida contém um anexo com a extensão .exe.
  2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio.

- 1. Condição: Uma mensagem de email recebida chega do seu patrão.
  2. Ação: Mover a mensagem para a pasta "Trabalho".

Recomendamos que você use uma combinação de regras nos programas antispam a fim de facilitar a administração e filtrar os spams com mais eficiência.

6.4.4.2 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceites, ou para os quais foi concedida permissão de acesso. O termo "lista de permissões de email" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de email, nomes de domínio ou endereços IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço IP não serão recebidas. Se a lista de permissões não for exclusiva, tais mensagens não serão excluídas, mas filtradas de algum modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

6.4.4.3 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições: as criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

O uso dessas listas de proibições é um componente essencial da filtragem antispam bem-sucedida, mas é muito difícil mantê-la, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos o uso de uma lista de permissões e uma lista de proibições para filtrar os spams com a maior eficácia.

6.4.4.4 Lista de exceções

A Lista de exceções geralmente contém endereços de email que podem ser falsificados e usados para o envio de spam. As mensagens de email de endereços relacionados na Lista de exceções serão sempre rastreadas quanto a spam. Por padrão, a Lista de exceções contém todos os endereços de email em contas existentes dos clientes de email.

6.4.4.5 Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os emails de spam em massa com base no número de mensagens recebidas e nas reações dos usuários. Cada mensagem deixa uma "marca" digital única com base no conteúdo da mensagem. O número de ID único não diz nada sobre o conteúdo do email. Duas mensagens idênticas terão marcas idênticas, enquanto mensagens diferentes terão marcas diferentes.

Se uma mensagem for marcada como spam, sua marca será enviada ao servidor. Se o servidor receber mais marcas idênticas (correspondendo a uma determinada mensagem de spam), a marca será armazenada no banco de dados de marcas de spam. Ao rastrear as mensagens recebidas, o programa envia as marcas das mensagens ao servidor. O servidor retorna as informações sobre que marcas correspondem às mensagens já marcadas pelos usuários como spam.

7. Dúvidas comuns

Este capítulo contém algumas perguntas e problemas mais freqüentes encontrados. Clique no título do capítulo para descobrir como solucionar o seu problema:

Se o seu problema não estiver incluído na lista das páginas de ajuda acima, tente pesquisar nas páginas de ajuda do ESET Smart Security.

Se não conseguir encontrar a solução para o seu problema/pergunta nas páginas de ajuda, poderá acessar nossa Base de conhecimento ESET on-line, atualizada regularmente. Links para nossos artigos mais populares na Base de conhecimento estão incluídos abaixo para ajudá-lo a resolver problemas comuns:

Recebi um erro de ativação durante a instalação do meu produto ESET. O que isso significa?
Como posso digitar meu Nome de usuário e Senha no ESET Smart Security/ESET NOD32 Antivírus?
Eu recebo a mensagem de que minha instalação ESET terminou prematuramente
O que eu preciso fazer depois de renovar minha licença? (Usuários Home)
E se eu mudar o meu endereço de email?
Como iniciar o Windows em modo de segurança ou Modo de segurança com rede

Se necessário, você pode entrar em contato com nosso Atendimento ao cliente com as suas perguntas ou problemas. O formulário de contato pode ser encontrado na guia **Ajuda e Suporte** do ESET Smart Security.

7.1 Como atualizar o ESET Smart Security

A atualização do ESET Smart Security pode ser executada de forma manual ou automática. Para acionar a atualização, clique em **Atualizar agora** na seção **Atualização**.

A instalação padrão cria uma tarefa de atualização automática que é executada a cada hora. Se precisar alterar o intervalo, acesse **Ferramentas** > **Agenda** (para obter mais informações sobre a Agenda, clique aqui).

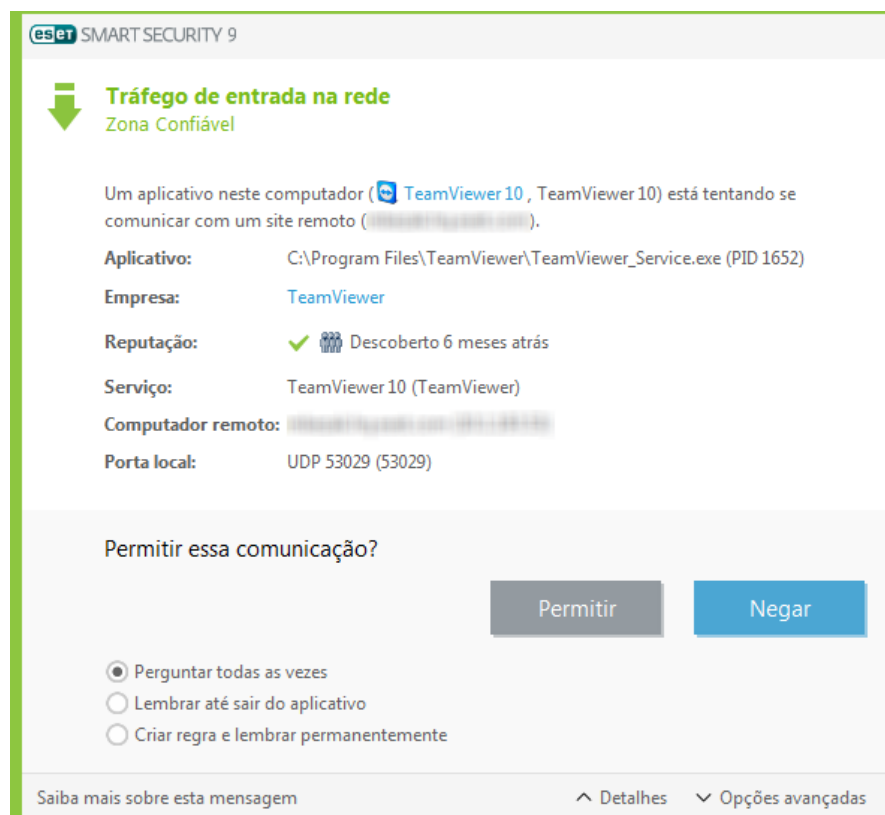
7.2 Como remover um vírus do meu PC

Se o seu computador estiver mostrando sintomas de uma infecção por código malicioso, como, por exemplo, estiver mais lento, congelar com frequência, recomendamos que você faça o seguinte:

1. Na janela do programa principal, clique em **Rastrear o computador**.
2. Clique em **Rastrear seu computador** para começar o rastreamento do sistema.
3. Após a conclusão do rastreamento, revise o log com o número de arquivos verificados, infectados e limpos.
4. Se desejar verificar se há vírus em apenas uma certa parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados em busca de vírus.

Para informações adicionais consulte nosso artigo na Base de conhecimento ESET atualizado regularmente.

7.3 Como permitir comunicação para um determinado aplicativo

Se uma nova conexão for detectada no modo interativo e se não houver uma regra correspondente, será solicitado que você permita ou negue a conexão. Se desejar executar a mesma ação toda vez que o ESET Smart Security tentar estabelecer conexão, marque a caixa de seleção **Lembrar ação (criar regra)**.

Você pode criar novas regras do firewall pessoal para aplicativos antes de eles serem detectados pelo ESET Smart Security na janela de configuração do firewall pessoal, localizada em **Rede** > **Firewall pessoal** > **Regras e zonas** > **Configuração**. Para que a guia **Regras** esteja disponível em **Configuração de zona e regra**, o modo de filtragem do firewall pessoal deve ser definido como Modo interativo.

Na guia **Geral**, insira o nome, a direção e o protocolo de comunicação para a regra. A janela permite que você defina a ação a ser tomada quando a regra for aplicada.

Insira o caminho para o executável do aplicativo e a porta de comunicação local na guia **Local**. Clique na guia **Remoto** para inserir o endereço remoto e a porta (se aplicável). A regra recém-criada será aplicada assim que o aplicativo tentar comunicar novamente.

7.4 Como habilitar o Controle dos pais para uma conta

Para ativar o Controle dos pais para uma conta de usuário específica, siga estas etapas:

1. Por padrão, o Controle dos pais está desabilitado no ESET Smart Security. Há dois métodos para ativar o Controle dos pais:
   - o Clique em em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** na janela principal do programa e altere o estado do Controle dos pais para ativado.
   - o Pressione F5 para acessar a árvore de **Configuração avançada**, vá para **Web e email** > **Controle dos pais** e em seguida selecione a opção ao lado de **Integrar ao sistema**.
2. Clique em **Configuração** > **Ferramentas de segurança** > **Controle dos pais** na janela principal do programa. Mesmo que **Ativado** apareça ao lado de **Controle dos pais**, você deverá configurar o Controle dos pais para a conta desejada clicando em **Proteger esta conta**. Na janela de configuração da Conta, insira uma idade para determinar o nível de acesso e as páginas da web recomendadas para a faixa etária informada. O Controle dos pais agora será

ativado para a conta de usuário especificada. Clique em **Conteúdo permitido e proibido...** em um nome de conta para personalizar categorias que você deseja permitir ou bloquear na guia Categorias. Para permitir ou bloquear páginas da web personalizadas que não correspondam a uma categoria, clique na guia Exceções.

7.5 Como criar uma nova tarefa na Agenda

Para criar uma nova tarefa em **Ferramentas** > **Agenda**, clique em **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os arquivos de log também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de log para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um snapshot do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, explicaremos a seguir como adicionar uma nova tarefa de atualização:

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Insira o nome da tarefa no campo **Nome da tarefa** e clique em **Próximo**. Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Acionado por evento.** Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As opções disponíveis são:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução (horas)**)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida. Clique em **Concluir** quando tiver concluído as alterações.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo. que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **Concluir** e a nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

7.6 Como agendar um rastreamento semanal do computador

Para agendar uma tarefa regular, abra a janela do programa principal e clique em **Ferramentas** > **Agenda**. A seguir está um pequeno guia sobre como agendar uma tarefa. Essa tarefa criará um rastreamento nas unidades locais a cada 24 horas. Visite nosso artigo da Base de conhecimento para informações mais detalhadas.

Para agendar uma tarefa de rastreamento:

1. Clique em **Adicionar** na tela principal do módulo Agenda.
2. Selecione **Rastreamento sob demanda do computador** no menu suspenso.
3. Escolha um nome para a tarefa e selecione **Semanalmente** para a frequência da tarefa.
4. Configure a data e hora em que a tarefa será executada.
5. Selecione **Executar a tarefa tão logo quanto possível** para realizar a tarefa mais tarde se a tarefa programada não começar por qualquer motivo (por exemplo, o computador estava desligado).
6. Revise o resumo da tarefa agendada e clique em **Fim**.
7. No menu suspenso **Alvos**, selecione **Unidades locais**.
8. Clique em **Concluir** para aplicar a tarefa.